NT500 Offline
Getting Started Guide

STANLEY®
Security Solutions

Copyright © 2007 Stanley Security Solutions, Inc.
and Stanley Logistics, Inc.
All rights reserved.
Printed in the United States of America.

Information in this document is subject to change without notice and does not represent a commitment on the part of Stanley Security Solutions, Inc. The software described in this document are furnished under a license agreement or nondisclosure agreement.

This publication is intended to be an accurate description and set of instructions pertaining to its subject matter. However, as with any publication of this complexity, errors or omissions are possible. No part of this manual and/or databases may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose, without the express written permission of Stanley Security Solutions, Inc.

This document is distributed as is, without warranty of any kind, either express or implied, respecting the contents of this book, including but not limited to implied warranties for the publication's quality, performance, merchantability, or fitness for any particular purpose. Neither Stanley Security Solutions, Inc, nor its dealers or distributors shall be liable to the user or any other person or entity with respect to any liability, loss, or damage caused or alleged to be caused directly or indirectly by this publication.

The Best Access Systems logo is a registered trademark of Stanley Security Solutions, Inc.

Microsoft, Windows, CE, and ActiveSync are registered trademarks of Microsoft Corporation.

T81633/Rev – ER-7991-40 May 2007

Contents

1 Introduction

Related documents 1–2

Getting technical support 1–2

How to use this guide 1–2

2 Architectural Overview

NT500 sample applications 2–3

Software features 2–7

Components and connections 2–8

3 First-Time NT500 Offline System Installation & Setup

System requirements 3–2

Navigating the software 3–2

Installing the system 3–4

Defining the system 3–7

Setting up organization options 3–7

Creating time and mode profiles 3–17
Setting up hardware 3–26
Creating cardholders and operators 3–33
Configuring a lock using a laptop 3–40
Configuring an office admin kit as an enrollment station 3–43
Viewing events, diagnostic information, and reports 3–45
Database backup and restoration 3–49

Glossary of Terms

Terms A–2

Chapter 1

Introduction

Thank you for choosing the Stanley NT500 Security Management System. The Stanley NT500 System allows a wide variety of institutions (educational, retail, health care, property management, and so forth) to secure access control of interior and perimeter doors. The Stanley NT500 System sets new standards for performance flexibility and ease of use.

The Stanley NT500 System software works with approved Windows® operating systems. See your Stanley Security Solutions representative for details.

In this guide you will find an overview of some typical applications of the NT500 System. You also will find step-by-step guidance for using the basic offline features of the NT500 System software.

Notes

Related documents

The following documents are available to help you install, maintain, and operate components of the NT500 System. See your Stanley Security Solutions Representative for more information.

- (T81149_14100) *AC302 Access Controller Quick Start Guide*
- (T81150_14101) A*C500 Access and Alarm Server Quick Start Guide*
- (T81151_14102) *AC512 Access Controller Quick Start Guide*
- (T81152_14103) *AC520 Input Controller AC530 Output Controller Quick Start Guide*
- (T81153_14104) *Designer and Vandal-Resistant Readers Installation Guide*
- (T81635) *Installation Instructions for 93KN Cylindrical Locks*
- (T81636) *Installation Instructions for 45HN Mortise Locks*
- (T81637) *Installation Instructions for EXN Exit Trim Locks*
- (T81634) *NT500 Transport Guide*
- (T81154_14105) *PC Interface Kit Installation Guide*
- (T81155_14106) *Power Supply DIN Rail Mounting Installation Guide*
- (T81157_14108) *Replacement Power Supply for Boxed Controllers Installation Guide*
- (T81158_14109) *Replacement PCB for Boxed Controllers Installation Guide*

Getting technical support

Stanley Security Solutions Representatives provide technical support for the Stanley NT500 System. You may locate the representative nearest you by visiting us on the web at www.stanleysecuritysolutions.com.

How to use this guide

This manual is intended for use as a reference guide when using the Stanley NT500 System software in offline mode.

Chapter 2, Architectural Overview – This chapter provides an overview of the Stanley NT500 online and offline worlds.

Chapter 3, First-time System Configuration & Installation – This chapter provides complete step-by-step instructions for the proper setup of a new offline system.

Appendix A, Glossary – This appendix provides a list of terms that are used in the Stanley NT500 System software.

Chapter 2

Architectural Overview

The Stanley NT500 Security Management System can be thought of as having two general architectural models for addressing the security needs of most customer applications. These two models can be generally categorized as “online” and “offline” .

In offline mode, the Stanley NT500 System can manage readers, locks, and controllers.

The Stanley NT500 Security Management Suite comes in four models. The NT510 and NT520 systems are designed for basic access control of offline door management. The NT540 and NT550 systems are enhanced versions with additional online reader capability.

Notes

The table below outlines features of the NT500 Security Management Suite.

	NT510	NT520	NT540	NT550
Cardholders	5000	5000	10,000	75,000
Offline doors	Unlimited	Unlimited	Unlimited	Unlimited
Online doors		16	200	1000
Networked control via IP		Yes	Yes	Yes
Access and alarm server			Yes	Yes
Input/output control hardware			Yes	Yes
Software				
Badge design	Optional	Optional	Optional	Standard
Elevator control			Optional	Standard
CCTV/DVR control			Optional	Standard
Mustering			Optional	Standard
Number of Clients	1	5	5	10

In an online application, most access control decisions are performed by a component called a controller. The controller is a circuit board with on-board memory, and this on-board memory must be configured by users who understand access control functions and features.

The online configuration is accomplished through an operator entering data on or through a computer called a server. This server is a computer where the access control system database resides. An operator can enter configurations in the server database through the NT500 System software interface and these updates are sent over the computer network to the appropriate controllers.

When used offline, the same readers, locks, and controllers can be used with the NT500 System. Updates to the access parameters for a cardholder or door are made using a PDA or laptop connected directly to the affected lock. Offline use is most often the solution chosen for a site that does not need real time updates. Offline use also has lower up front costs.

The main focus of this guide is the offline use of the NT500 System software. Therefore, NT510 and NT520 system users are the primary audience for this guide.

NT500 sample applications

Notes

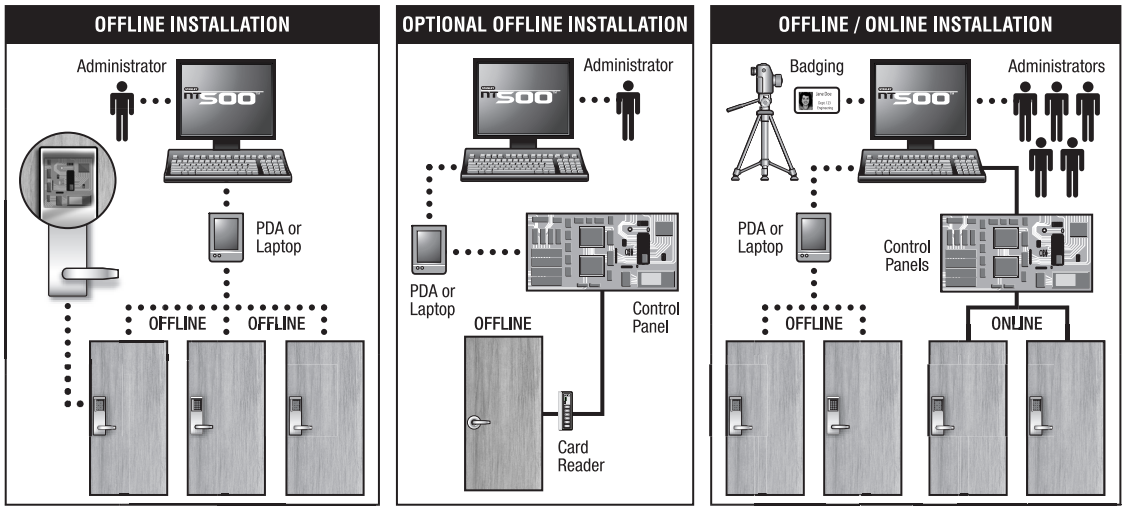
With the use of the NT500 System software, three basic access schemes can be developed. These include:

1) An offline system in which only the battery operated electronic lock's built in memory and/or door controllers (AC512B), along with NT500 System software are used. Access is defined in the NT500 System software, while events are recorded in the electronic lock's built in memory and/or door controllers. Such a system enables the administrator to take lock programming to the physical doors and to retrieve events from the locks.

2) An online system in which the door controllers (AC512IPB or AC512B) are used along with the NT500 System software. This enables the administrator to program the physical doors and to retrieve events from the locks while from a desktop computer. (The use of a two door controller (AC512IPB or AC512B) allows the control of magnetic locks, electric strikes, electric locks and other electric devices.)

3) A hybrid system with both online and offline functionality.

Figure 2.1 Applications of NT500



Notes

Scenario 1 — Hollow metal entrance door only

Your facility has two metal entrance/exit doors. You wish to allow employees and the public full access during business hours (from Monday through Friday 8:00 am to 6:00 pm). Both doors will be programmed with an unlock/relock schedule to make sure the doors are automatically unlocked during these hours. This unlock/relock schedule will be set to work with a "First Card" mode, meaning the doors will not unlock (via the schedule) until a token is presented from a valid cardholder. Outside of those specified hours and on weekends, only employees should have access to the entrance/exit doors. The definition of who needs access to the main entrance/exit doors only needs to be updated when new employees arrive or employees part with the company. Your site could have magnetic stripe locks, dual-validation or proximity type locks.

You will need NT500 locks and the NT500 System software to set up this type of access system. To set up this access system the use of hardwired door controllers (AC512IPB or AC512B) is not required. Definition of access for the entrance/exit doors during business hours and on weekends can be achieved through use of time mode profiles, door mode profiles, and access groups. Once you establish the appropriate profile relationships in the software, this information can be downloaded to the lock hardware at each door via a PDA using the NT500 Transport software or via a laptop computer. New employees can be issued cards for access as necessary and this information can also be updated via PDA using the NT500 Transport software or laptop.

Scenario 2 — Glass/aluminum entrance doors with overhead door and computer door

Your facility has two glass/aluminum entrance/exit doors that you wish to allow full access to the public and employees from Monday through Friday 8:00 am to 6:00 pm. Both doors will be programmed with an unlock/relock schedule to make sure the doors are automatically unlocked during these hours. This unlock/relock schedule will be set to work with a "First Card" in mode, meaning the schedule will not go into place until a token is presented from a valid cardholder. Outside of those specified hours and on weekends, only employees should have access to the entrance/exit doors. The

Notes

definition of who needs access to the main entrance/exit doors only need to be updated when new employees arrive or employees part with the company.

There is also an overhead dock/delivery door that you wish to have accessible only to specific employees with valid card access. This access will allow them to raise and/or lower the dock door.

The final area you wish to provide access security for is an IT room housing valuable computer equipment. This area should only be accessible to specific employees but those employees may have access 24 hours a day and 7 days a week.

You will need the NT500 System software and two door controllers (AC512IPB or AC512B) to set up this type of access system. Definition of access for the entrance/exit doors during business hours and on weekends can be achieved through use of time mode profiles, door mode profiles, and access groups set up in the software. This information can be downloaded to the controllers via an existing TCP/IP network or via a direct serial connection to a local computer. New employees can be issued cards for access as necessary and this information can also be updated via the TCP/IP or serial connection. You can view history events at anytime on the local computer.

Scenario 3 — Glass/aluminum entrance door with two interior doors

Your facility has one glass/aluminum entrance/exit door and two interior office doors. Full access to the public and employees is desired for the entrance/exit door from Monday through Friday 8:00 am to 6:00 pm, but only access by employees is desired for the interior office doors. The individuals who have access to the entrance/exit door change often and you want to log cardholder information about activity at this door. The cardholders and access for the two interior doors will change in-frequently.

You will need NT500 locks, the NT500 System software, and a door controller (AC512IPB or AC512B) to set up this type of access system. Definition of access for the entrance/exit doors during business hours and on weekends can be achieved through use of time mode profiles, door mode pro-

Notes

files, and access groups. The door controller can be used for the entrance/exit door that will allow public access.

For the entrance/exit door, you will first want to establish the appropriate profile relationships with unlock/relock schedules and employee access, to grant access to only specific employees through the use of door mode profiles, time mode profiles, and access groups or individual cardholder access. Once you define these relationships in the software, this information can be downloaded to the controller via a TCP/IP or a serial connection from a local computer.

For the offline office doors, once you establish the appropriate profile relationships in the software this information can be downloaded to the lock hardware at each door via a PDA using the NT500 Transport software or via a laptop computer. New employees can be issued cards for access as necessary and this information can also be updated via PDA using the NT500 Transport software or laptop.

Software features

Notes

The following table compares the software features supported by the NT510 software license to those supported by the NT520 software license.

Software Features	NT510	NT520
Support for unlimited offline locks	✔	✔
Support for up to 16 online door controllers		✔
Up to 5000 cardholders per system	✔	✔
Up to 100 Time Zones	✔	✔
Up to 20 Holidays	✔	✔
Up to 100 Access Groups	✔	✔
Up to 1000 Access Groups		✔
Up to 5 simultaneous client connections		✔
User definable fields	✔	✔
Import/export capability user data	✔	✔
Optional card designer ad-on software module	✔	✔
Multi-language support	✔	✔
Communication with offline locks and controllers directly via PC/Laptop or PDA	✔	✔
Ability to create cardholder and lock profiles by copying and editing existing profiles.	✔	✔

Notes

Components and connections

The following hardware and software components are used to create an offline Stanley NT500 System:

- Stanley NT500 System software
- Dedicated computer, see your Stanley Security Solutions representative for complete details
- NT500 Locks, cylindrical (93KN), mortise (45HN) or exit hardware trim (EXN) models available with proximity, magnetic stripe or dual validation reader
- Card encoder (optional for magnetic stripe)
- Access cards (proximity or magnetic stripe)
- Laptop or PDA
- Laptop cables
  - Null modem cable— connects laptop to offline lock programming cable (BASDCAB)
  - Offline lock programming cable — connects null modem cable to offline lock/controller
- PDA cables
  - Serial cable (from PDA manufacturer) — connects PDA to offline lock programming cable
  - Offline lock programming cable — connects serial cable to offline lock/controller
  - PDA USB/Serial Autosync cable — connects PDA to PC.

Controllers

Notes

The following controllers can be used with an offline Stanley NT500 System (using NT510 or NT520 software). A controller dictates lock behavior according to defined parameters such as time, individual access rights, card presented to a reader, or activation of a Request to Exit switch.

- AC512 – The AC512 is a two-door controller that can manage up to two access points. This controller also allows for ADA compliance by supporting programmed extended access times.
- AC301 – The AC301 is a single-door, battery-powered controller. This controller works with both mortise, cylindrical, and exit hardware trim.

Encoders

The type of readers and access cards used in your access system will dictate the type of encoders needed.

For magnetic stripe encoding an MSR206 Magnetic Stripe Card Writer can interface with the NT500 System software. NT500 System users can purchase HID or Indala proximity cards that come pre-programmed.

Readers

A reader sends a code to the controller when a card is presented or PIN entered. If valid access information is presented an unlock signal is sent to the door. Most readers will illuminate a green LED to indicate to the cardholder that access is granted or a red LED to indicate that access is denied. Some readers are stand alone and some are integrated into the AC301 Lock.

The following readers can be used with an offline Stanley NT500 System.

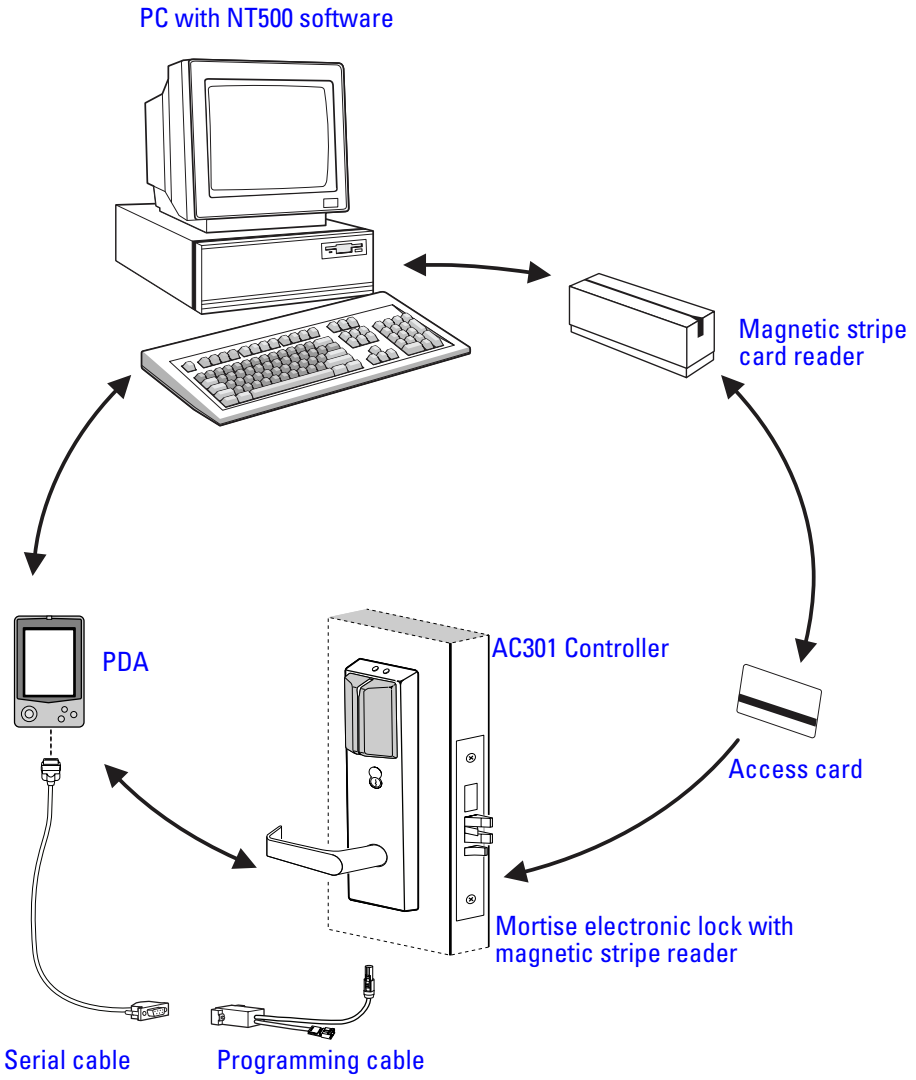
- HID Proximity
- Indala Proximity
- Magnetic Stripe
- Dual Validation (magnetic/keypad)

Notes

PDAs and Laptops

PDAs and Laptops are used with an offline NT500 System to transfer configuration information from the PC upon which the management software is installed to the lock and transfer history information from the lock to the PC.

Figure 2.2 Components and connections



Not shown:

- Laptop
- Cylindrical magnetic stripe electronic lock
- Mortise and cylindrical proximity electronic locks
- Mortise and cylindrical dual validation electronic locks
- Exit hardware trim
- AC512 Controller

Setup overview

In the next chapter you will find complete step-by-step instructions on the first time configuration of a Stanley NT500 System for offline use. Below is a brief outline of the main steps involved in the setup process and cross-references that will assist you in quickly finding this information.

- Navigating the software, see page 3-2.
- Installing the software, see page 3-4.
- Setting up Organizational Options, see page 3-7.
- Creating Time and Mode profiles, see page 3-17.
- Setting up the hardware, see page 3-26.
- Creating an Access Group, see page 3-31.
- Creating Cardholders and Operators, see page 3-33.
- Viewing Events, see page 3-45.

Notes

Notes

First-Time NT500 Offline System Installation & Setup

You are now ready to start setting up your Stanley NT500 offline system. The tasks described in this chapter do not include the installation of the locks themselves. The installation of locks that can be used with the Stanley NT500 System (93KN, 45HN, EXN) is fully described in the installation instruction documents listed below. Contact your Stanley Security Solutions Representative for a copy of these documents.

Title	Document no.
Installation Instructions for 93KNCylindrical Locks	T81635
Installation Instructions for 45HN Mortise Locks	T81636
Installation Instructions for EXN Exit Trim Locks	T81637

Notes

System requirements

Before installing the Stanley NT500 System software, it is important to confirm that your computer infrastructure meets the minimum system requirements. See you Stanley Security Solutions Representative for more information.

Navigating the software

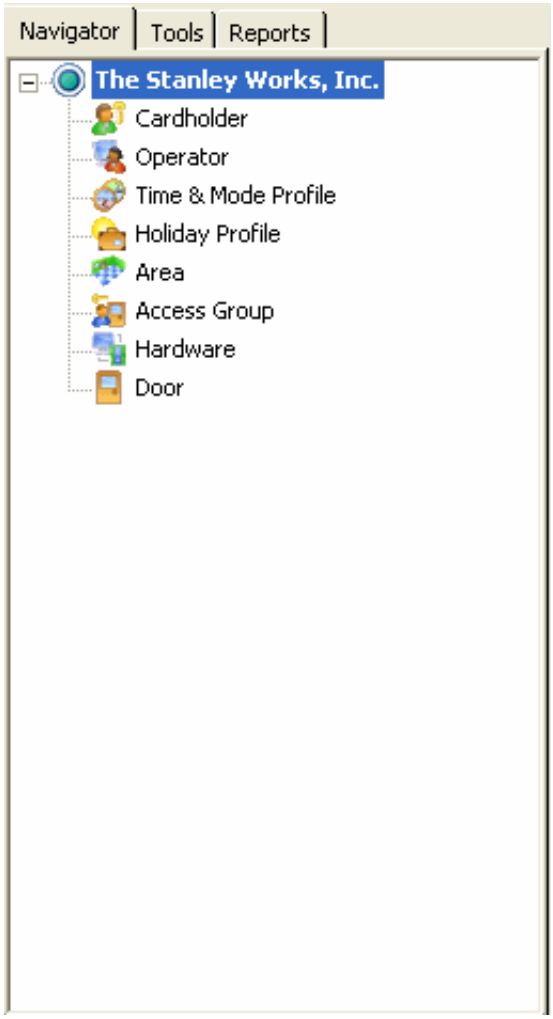
The Stanley NT500 System software follows Windows® conventions. Therefore both menus and toolbars are available for navigation through the software. The icon toolbar is context sensitive. The various icon toolbars are illustrated in Figure 3.1. Help for a particular topic can be viewed by clicking on an icon or field and pressing F1. The Explorer Bar appears on the left side of the main screen. The Explorer Bar tabs are useful for navigating to the most commonly used functions. The Explorer Bar is composed of a Navigator, Tools, and Reports tab (see Figure 3.2). The majority of system definition tasks can be initiated by clicking the icons on the appropriate Explorer Bar tab.

Figure 3.1 Menus and toolbars

Navigator tab menu and toolbar

Tools and Reports tab menu and toolbar

Figure 3.2 Explorer bar



Notes

Notes

Installing the system

Make sure that you have the following components before you start installing the Stanley NT500 System:

- Stanley NT500 System software
- Dedicated computer, see your Stanley Security Solutions Representative for complete details
- NT500 Locks, cylindrical (93KN), mortise (45HN) or exit hardware trim (EXN) models available with proximity magnetic stripe or dual validation reader
- Card encoder (optional for magnetic stripe)
- Access cards (proximity or magnetic stripe)
- Laptop or PDA
- Laptop cables
  - Null modem cable— connects laptop to offline lock programming cable (BASDCAB)
  - Offline lock programming cable — connects null modem cable to offline lock/controller
- PDA cables
  - Serial cable (from PDA manufacturer) — connects PDA to offline lock programming cable
  - Offline lock programming cable — connects serial cable to offline lock/controller
  - PDA USB/Serial Autosync cable — connects PDA to PC.

Installer privileges

The Stanley NT500 System software can only be installed by a user with Administrator privilege. It is strongly recommended that the Administrator take measures to assure the software cannot be accidentally deleted from the PC.

Types of installation

Two types of installation are possible with the NT500 installation CD—full (server) or “client-only” .

For stand alone systems, the full installation should be run. A full installation includes both client and server elements. The server part contains the database and server software, and communicates with the control panel. The client part is the user interface.

A client-only installation lets you run the user interface from a different computer than the one this software was originally installed upon, via your local area network. However, you will not be able to connect to a lock with the “client-only“ installation. When you perform a client-only installation you specify the name of the computer that contains your full installation. This can be changed later if required.

Before installing the Stanley NT500 software, also make sure that you have completed the following:

☐ Determine whether your database will use Microsoft® SQL Server, or MSDE.

The Microsoft® SQL Server Desktop Engine (MSDE) must be installed on your PC before the Administration Software. If it is not, the opportunity to install it is displayed before the software options are displayed.

All prerequisite software is supplied on the CD and must be installed first. The setup program checks if the software is already present on you computer, and allows you to install it if the prerequisite software is not detected.

Notes

To install the software

1 Insert the CD into the CD drive of the PC.

When the CD is placed in the CD drive of the PC the following options are available:

- *Activate DotNet Framework™ V1.1 (grayed out if already installed).*
- *Install Windows® Message Queuing (grayed out if already installed).*
- *Install MSDE Database™ (grayed out if already installed).*
- *Install Crystal Reports™ 11 (grayed out if already installed).*
- *Install Microsoft® Web Service Extensions (WSE, grayed out if already installed).*
- *Start Installation.*
- *Obtain and install license file (not required for NT510).*

2 Follow the Setup Wizard prompts and accept the license agreement.

3 Make a note of any existing license keys. New software versions may require a new version key.

For details on obtaining a license key see page 3-49.

A shortcut is placed on the desktop.

During installation you will be asked to identify an access type. This parameter can be defined after installation but must be defined before adding doors and cardholders. We recommend assigning access based on areas (not doors) and based on groups rather than security levels. This access type is suggested because it allows you to add online functionality

Notes

later if the needs of your site change. For more information about access types see page 3-13.

To set a new password

When first signing into the application the default username (installer) and password (installer) should be updated.

1 Double click the Stanley NT500 desktop icon.
The Login screen appears.

2 In the Login Name field, type the default login name.

3 In the Password field, type the default password.

4 Click Log On.
You are prompted to enter a new password.

5 Enter and confirm the new password.

6 Click OK.

Defining the system

Notes

Overview

It is best to take time to plan what doors, time profiles, and individuals need to be included in your access management scheme.

To define an NT500 system, you need to configure:

- ☐ Organization options
- ☐ Time and mode profiles
- ☐ Hardware
- ☐ Access groups
- ☐ Cardholders
- ☐ Operators

Setting up organization options

Card format

After successful software installation, the first task in setting up your access control scheme is to define the card formats used at your site. The term card is used in this guide to refer to cards, tokens, or fobs, all of which can be presented to a reader to unlock the door. The card must be valid (known to the system, allow access to the area and not presented outside a permitted time profile).

The card format you use is determined by the type of readers in your access system (proximity, magnetic stripe, or dual validation).

To define the card formats for your system

1 From the Welcome Screen, select Set Organization Options or Tools > Options on the Main menu.

The Organization Options window appears.

2 From the left side of the Organization Options window, highlight Card Format.

3 Click Add

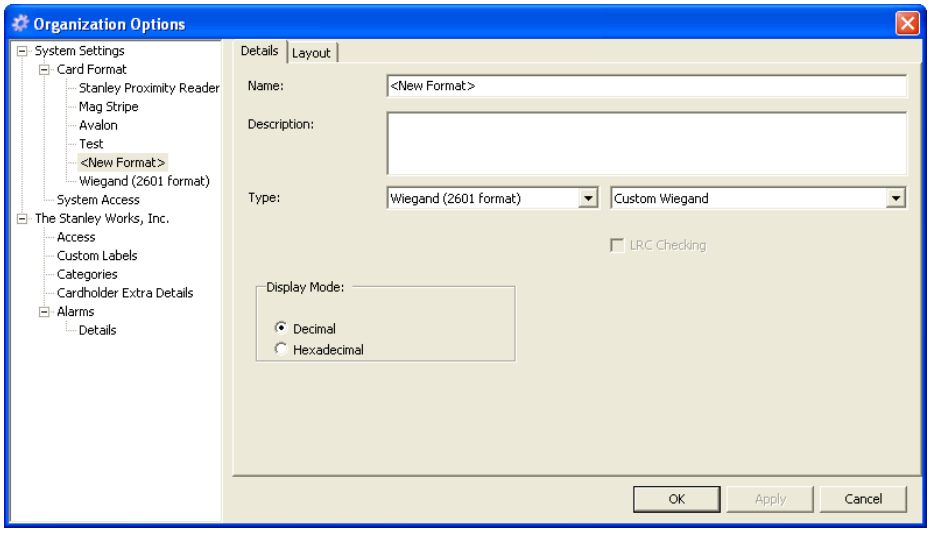
A warning message may appear notifying you that changing the card format order affects the way cards are interpreted and will require a database download to all control panels.

Notes

4 *Click OK.*

The New Format window appears.

Figure 3.3 Adding a new card format



5 In the Name field, enter a name for the card format.

6 In the Description field, enter a description of the card format.

A popular naming scheme is to use the name of your company or department.

7 In the Type field, select the card type by using the drop-down list.

8 Using the radio buttons, select the appropriate display mode.

9 Check the LRC Checking box if readers should validate the longitudinal redundancy check.

If the lock should not validate the LRC, make sure this check box is not checked.

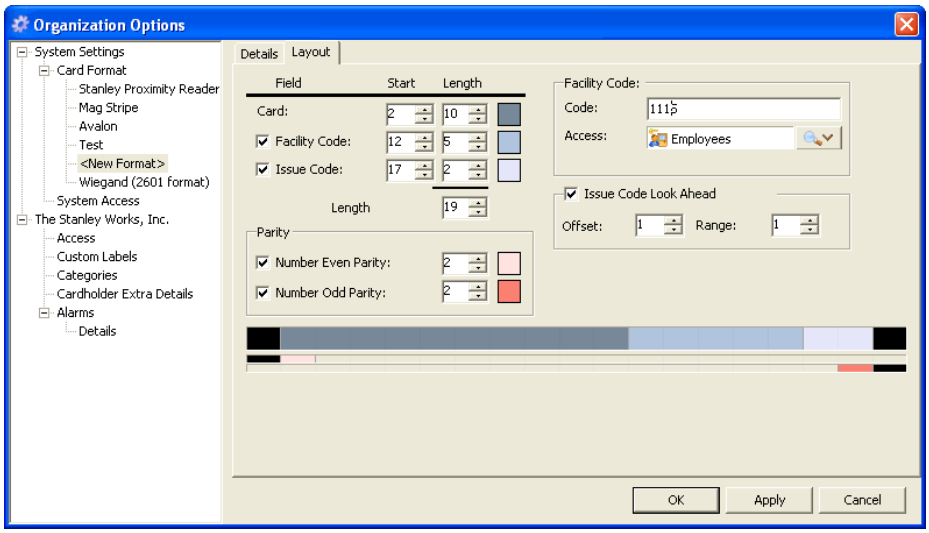
You can determine whether the locks using this configuration validate the longitudinal redundancy check (LRC). However, always validate the longitudinal redundancy check unless a Stanley Security Solutions Representative informs you otherwise. The LRC feature is included in most card formats and helps verify that the locks read the card data or PIN correctly.

10 For a proximity or Wiegand card format, Click OK.

For magnetic stripe or custom Wiegand card format definition continue with the following steps.

1 Click the Layout tab.

Figure 3.4 New card format-Layout tab



For magnetic stripe or custom Wiegand card format, the following details must be provided.

Card length: The card length is the total amount of information encoded on each access card.

Facility code format: A facility code generally is a unique sequence of digits that is programmed into every device and encoded on every access card that belongs to the facility. Check with your System Administrator to locate the facility code. When you define the facility code format, you indicate:

- the maximum number of digits in the facility code
- the starting location of the facility code on the access cards.

Card number/access code format: A card number or access code is a unique sequence of digits that identifies a user. When you define the card number or access code format, you indicate:

- the maximum number of digits in the card number or access code
- the starting location of the card number on the access cards.

Issue code format: An issue code generally indicates how many times an access card with a particular card number has been issued. For example, when an access card is first issued to someone, it normally is encoded with Issue 1. If the access card is damaged, lost, or stolen, and a replacement card is issued to the card holder, the card normally would be encoded with Issue 2.

Notes

Notes

When you define the issue code format, you indicate:

- the maximum number of digits in the issue code
- the starting location of the issue code on the access cards
- the range of issue codes that the device should accept.

2 In the Card Number Length field, type the number of digits (from 1 to 9) in the card number.

3 In the Card Length field, type the total number of digits of data (from 1 to 99) on the access cards or in the personal identification numbers (PINs), preceded by a zero if necessary. For example, if there are 20 digits of data on the access cards or in the PINs, type **20**.

4 If the card format includes a facility code, check the Facility Code checkbox.

a) In the Facility Code Location field, type the starting location (from 1 to 99) of the facility code, preceded by a zero if necessary. For example, if the facility code starts at position 3, type **03**.

b) In the Facility Code Length field, type the maximum number of digits (from 0 to 9) in the facility codes for this card format. For example, if the maximum facility code length is four digits, type **4**.

If you type 0, the devices using this configuration will not check the facility code when determining whether to grant access to a card.

When facility codes are used, you may indicate if an entire access group should have the facility code information applied to cardholder's within that group. This feature can be enabled using the drop-down list on the right side of the screen under Facility Code.

5 If the card format includes an issue code, check the Issue Code checkbox.

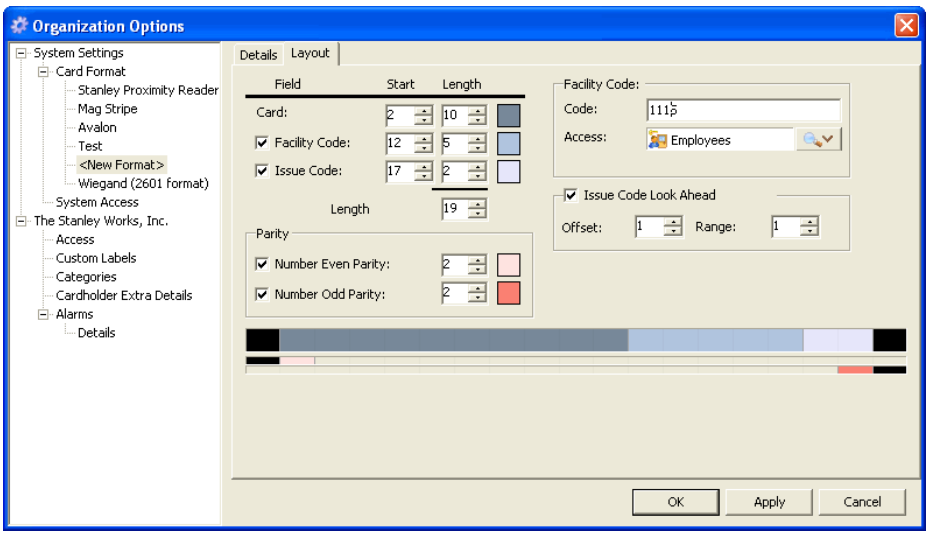
a) In the Issue Code Start field, type the starting location (from 1 to 99) of the issue code, preceded by a zero if necessary.

b) In the Issue Code Length field, type the number of digits (from 0 to 4) in the issue code for this card format. If you type 0, the devices will not check the issue code when determining whether to grant access to a card.

A total is calculated as the sum of the Card Length, Facility Code Length, and Issue Code Length.

The bar at the bottom of the window indicates the card format information locations and lengths.

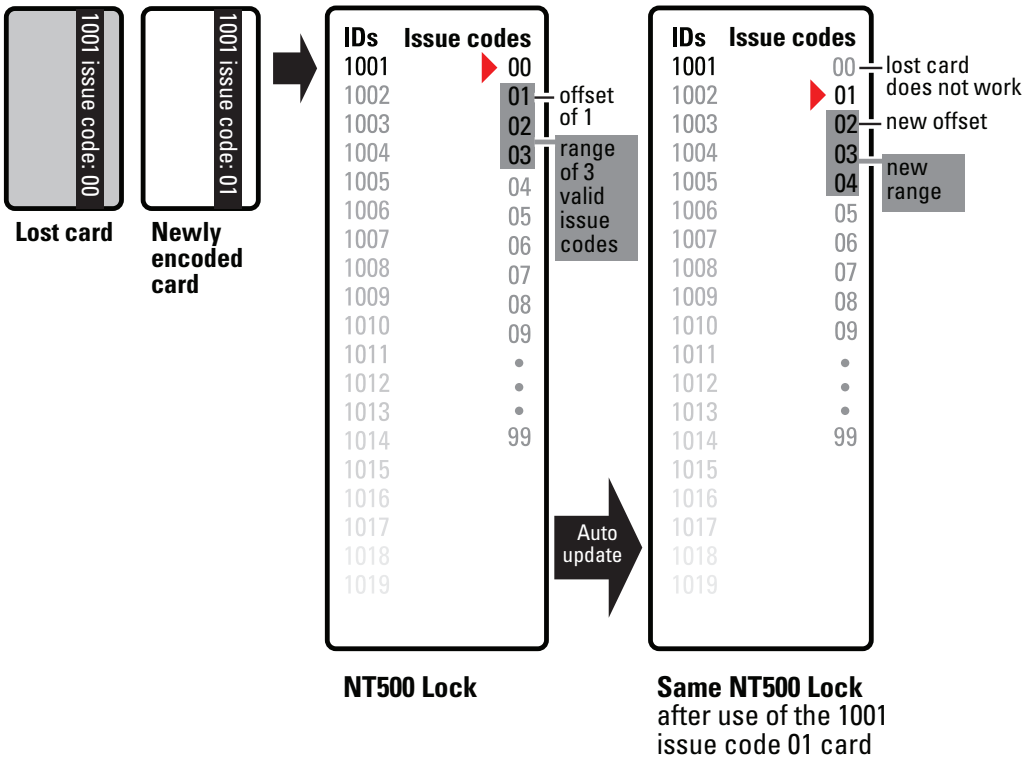
Figure 3.5 New card format-Layout tab



6 If the issue code look ahead feature is desired, check the Issue Code Look Ahead check box.

The following figure illustrates how the look ahead and issue code features are applied.

Figure 3.6 Issue code look ahead feature



Notes

Notes

The look ahead feature lets you program a magnetic stripe reader to accept an access card whose encoded issue code is higher than the current issue code recorded for the card in the lock's database. The setting for the look ahead feature determines how many numbers higher the access card's encoded issue code can be than the issue code on record for the card.

For example, if you enter 2 as the look ahead setting in a device's configuration, the device will accept an access card whose encoded issue code is one or two numbers higher than the issue code on record for the card (as long as the issue code is within the acceptable issue code range). The device would accept an access card whose encoded issue code is 3, even if the current issue code on record for the card is 1.

When the device accepts an access card with an encoded issue code different from the current issue code on record for the card, the device automatically updates its records to reflect the encoded issue code.

7 Enter an offset value.

This value will be added to the issue code when the New Issue button on the Cards tab of Cardholder window is selected.

8 Enter a range value.

The range represents the highest-numbered issue code that the devices should accept. The devices will reject any card with issue codes higher than this number.

*For example, if the devices should reject any card with an issue number higher than 8 and the issue code for the selected card format has one digit, type **8**.*

9 If the card format includes an even number parity bit, click the Number Even Parity checkbox.

10 If the card format includes an odd number parity bit, click the Number Odd Parity checkbox.

11 Click OK.

The new card format is included in the Card Format list on the left side of the window.

After defining card format(s) the system access must be defined.

System access

When assigning access it is best to use the access by area functionality if there is a desire or potential that the access system will be expanded to use online functionality in the future.

This guide will follow the path of defining access based on areas and access groups. This is the preferred method for defining access because it allows for future migration to Stanley NT500 online functionality.

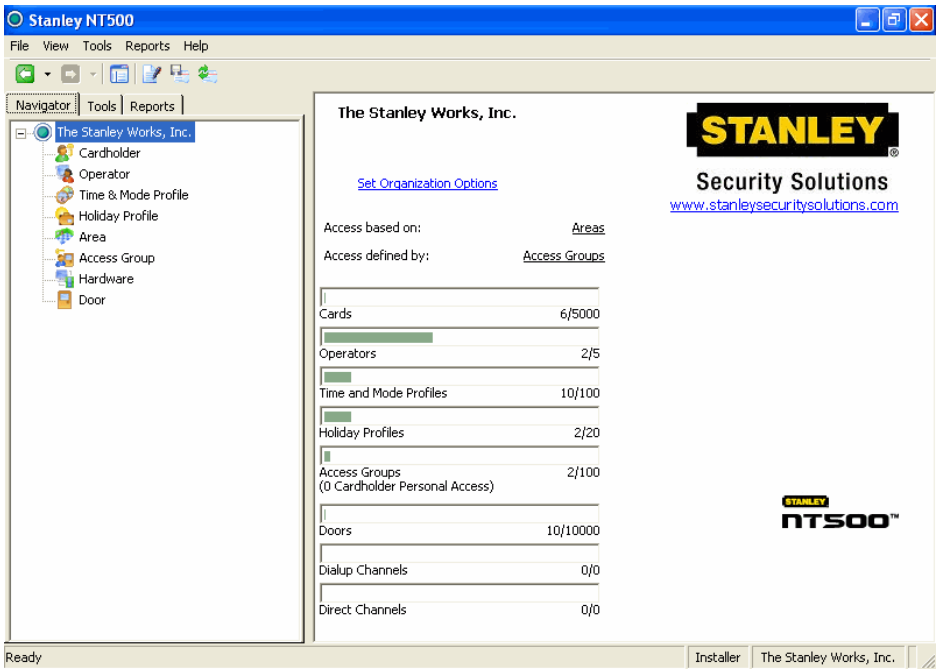
Caution: If access is assigned based on areas, an existing offline database can be migrated to interact with online components. If access is assigned based on doors and later you wish to take your access control system online, the database will not be maintained. All door, area, time and mode profile and cardholder information will have to be re-entered into the Stanley NT500 database. Security levels are generally reserved for assigning access to specific badges rather than assigning access privileges to doors over time.

The Welcome Screen is displayed after you first login, or when the company name is selected on the Explorer Bar's Navigator tab. The Welcome Screen displays information on the system (for example, number of cardholders and maximum limits of the system). If the operator privileges allow, it also has a Set Organization Options link that allows the modules to be customized. Setting system access can be initiated from the Welcome Screen.

Notes

Notes

Figure 3.7 Welcome screen

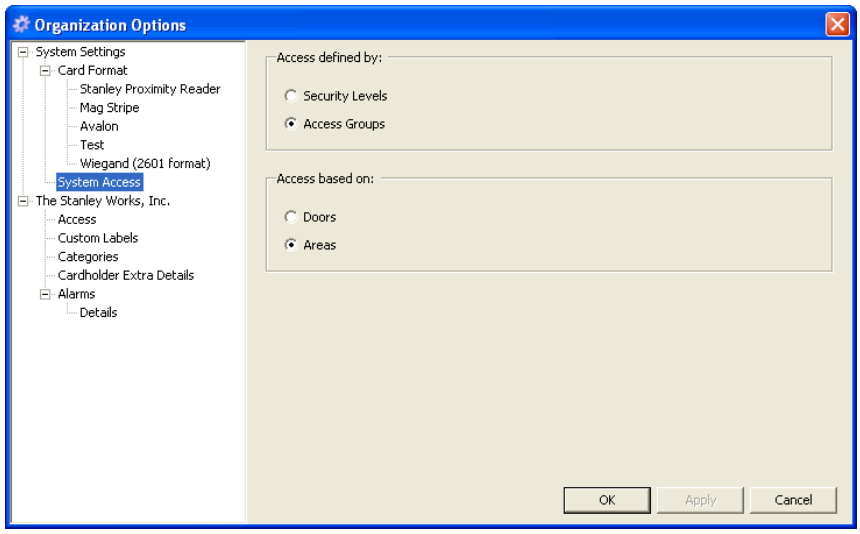


To define system access

1 From the Welcome Screen, select Set Organization Options or from the main menu select Tools > Options.

The Organization Options window appears.

Figure 3.8 Organization Options - System Access



2 Select System Access

The following options are presented:

Access defined by:

- Security Levels
- Access Groups

Access based on:

- Doors
- Areas

3 Click the appropriate radio button to select an access option.

4 Click Apply.

5 Click OK.

Access type options

The administration software may provide the following access type options:

Areas and access groups: Each cardholder is assigned to access groups that allow access to certain areas. For example, this option is used in systems where there is more than one door into most areas and a large number of areas that require grouping according to who has access. ***This is the recommended option for most NT500 System users.***

Areas and security levels: Each cardholder and area are assigned a security level which determines which areas each cardholder can access. For example, this option is used in systems where there is more than one door into most areas and a small number of areas. [NOT RECOMMENDED]

Doors and security levels: Each cardholder and door are assigned a security level which determines which doors each cardholder can open. For example, the option is used in systems where there is only one door into each area and a small number of areas. [NOT RECOMMENDED]

Doors and access groups: Cardholders are assigned to access groups that allow access to certain doors. For example, this option is used in systems where there is only one door into each area and a large number of areas that require grouping according to who has access.

The access type required is specified at installation but can be changed using customization. [NOT RECOMMENDED]

Notes

Notes

Organization information

At installation the application will prompt the user to enter organization information such as name, description, day to define as start of week, time zone, and default card format. Organization information can be added or modified using the following steps.

To add organization information

1 From the Welcome Screen, select Set Organization Options or from the main menu select Tools > Options.

The Organization Options window appears.

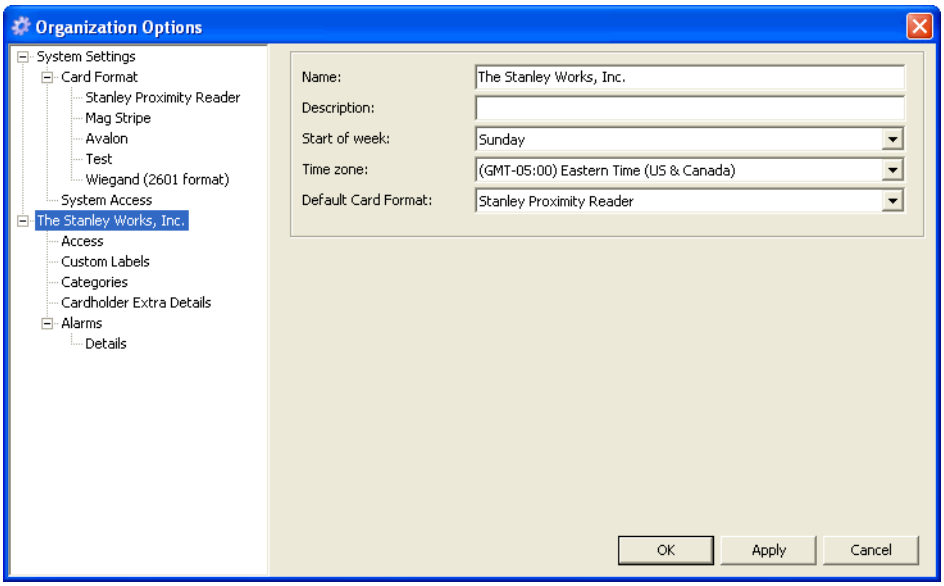
2 Select the organization name.

3 Edit the following fields as necessary.
- Name
- Description
- Start of week
- Time zone
- Default card format

4 Click Apply.

5 Click OK.

Figure 3.9 Adding organization information



Creating time and mode profiles

Time profile

A time profile consists of one or more time periods that can span multiple days. A time profile can be applied to an area, door, cardholder, or access group. A time profile dictates access during certain times (for example, only during office hours).

To create a time profile

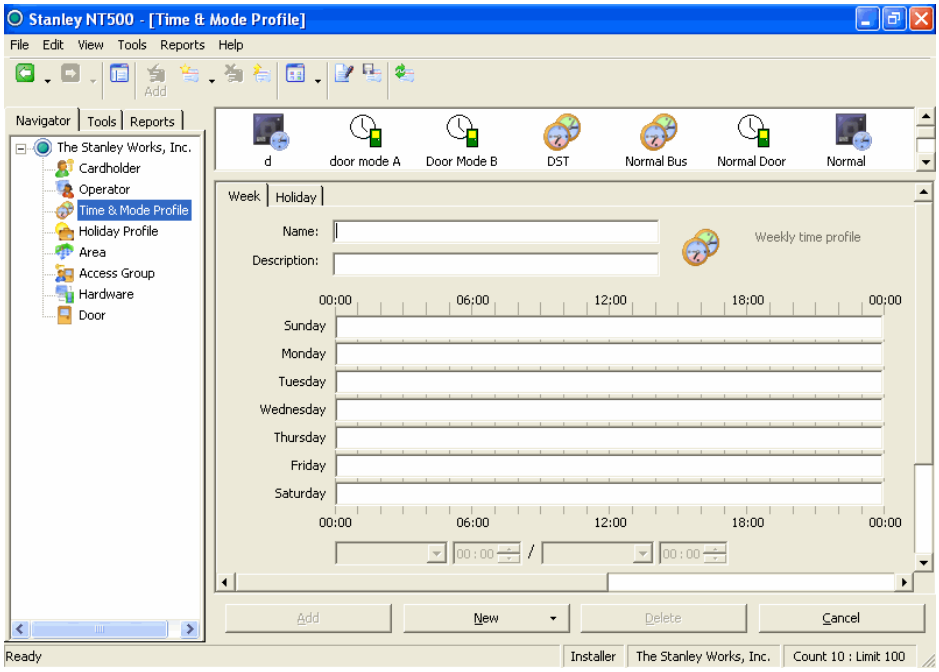
1 From the Explorer Bar's Navigator tab, click the Time & Mode Profile icon.

2 From the main menu, click Edit > Create New Record.

3 Click Create New Simple Time Profile.

The Time Profile window appears.

Figure 3.10 Time profile window



4 In the Name field, enter a name for the time profile.

5 In the Description field, enter a description of the time profile.

For example, a weekend time profile might be named *Summer Weekends* with a description of *Weekend hours (12-4 p.m.)*.

Notes

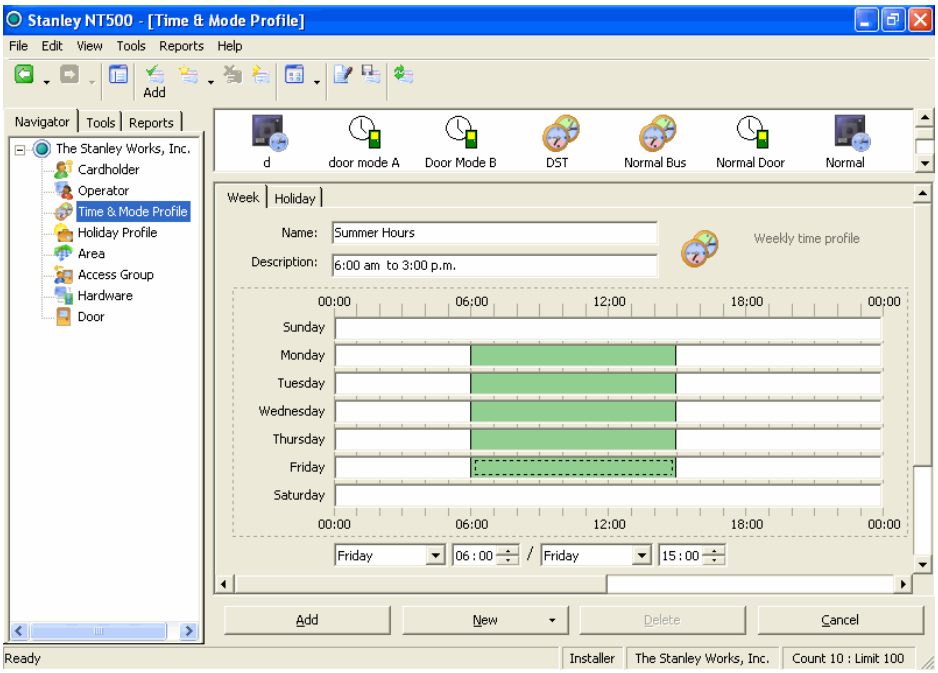
Notes

6 The hours of access defined by this time profile can be selected by clicking in the white field next to each weekday label. Then, while holding down the left mouse button, highlight the range of desired times.

7 Click Add.

A new time profile icon appears at the top of the screen.

Figure 3.11 Creating a time profile



To update a time profile

1 Select an existing time profile.

The Time Profile window appears.

2 On the Week tab, edit the desired fields.

3 Click Update to save your changes.

To delete a time profile

1 Select an existing time profile.

2 Click Delete.

3 Click OK to confirm.

The icon for the time profile you deleted is no longer displayed in the window.

Once time profiles have been created they may be applied to cardholders or access groups.

Holiday profile

A holiday profile can be assigned to a time profile to limit access during specified dates and times. First, a holiday profile must be defined, then it can be applied to a time profile.

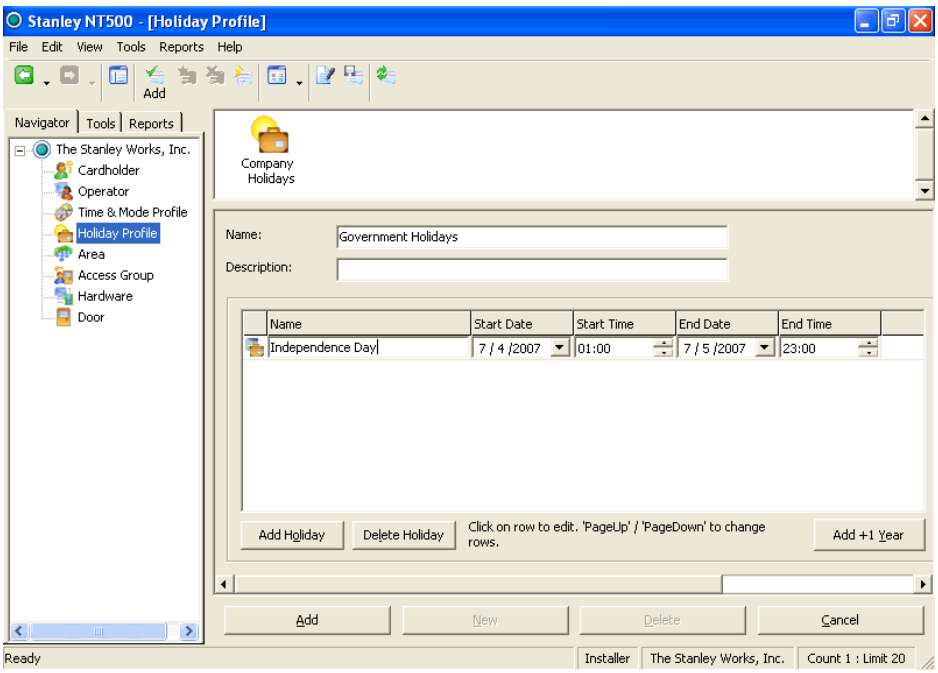
To define a holiday profile

1 From the Explorer Bar's Navigator tab, click the Holiday Profile icon.

2 Click New.

The Holiday Profile window appears.

Figure 3.12 Defining a holiday profile



3 In the Name field, enter a name for the holiday profile, such as Government Holidays.

4 In the Description field, enter a description of the holiday profile.

5 Click Add Holiday.

The Holiday Profile window appears.

6 In the Name column, enter a name for a specific holiday, such as Independence Day.

7 Edit the following fields by using the drop-down lists or typing directly into each field.

- Start Date
- Start Time
- End Date
- End Time

Notes

Notes

8 Click Add.

9 Repeat steps 5 through 8 for additional holidays to be included in this profile.

10 Click Update when all additional holidays to be included in the profile have been defined.

To apply a holiday profile to an existing time profile

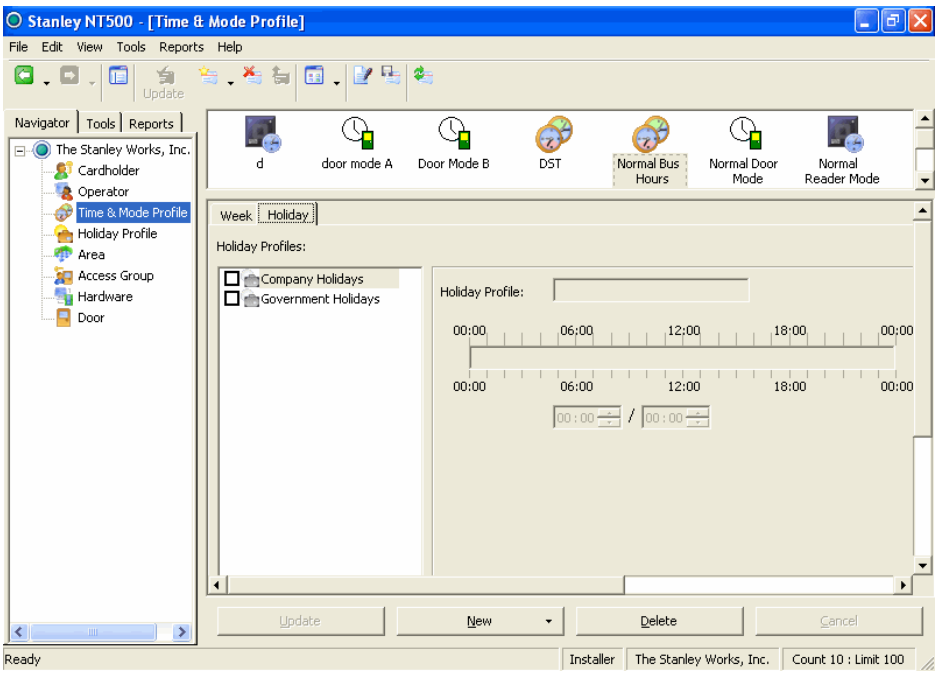
1 Select an existing time profile.

The Time Profile window appears.

2 Select the Holiday tab.

A list of available holiday profiles appears on the left side of the window.

Figure 3.13 Applying a holiday profile



3 Click the box next to the holiday(s) you want to apply to the time profile.

A check mark appears next to holiday profiles you select and will be applied to the time profile.

4 Click Update.

To delete a holiday profile

1 Select a holiday profile.
The Holiday Profile window appears.

2 Click Delete.

3 Click OK to confirm.
The icon for the holiday profile you deleted is no longer displayed in the window.

To remove a holiday profile from an existing time profile

1 Select a time profile.
The Time Profile window appears.

2 Select the Holiday tab.
A check appears next to any holiday profile currently applied to the time profile.

3 Click the checkbox to deselect the holiday profile(s) that you do not want to apply to the time profile.

4 Click Update.

Notes

Notes

Door mode profile

When a time profile is applied to a cardholder (or access group) it determines when a cardholder has access through a door. When a mode profile is applied to a door or reader, it determines the door behavior/mode (for example, area armed or disarmed, door open or closed).

Door mode profiles offer the following mode options:

- **Secured (default)**: Door requires a valid access card to be presented before unlocking for entry into an area.
- **First key open:** Door remains locked until the first valid card is presented during the time profile. Firstkey open permissions may be assigned to the access group as an option. The door will then remain unlocked until the end of the time mode profile.
- **Open:** Door remains unlocked until the time profile ends.
- **Bolted:** All cards will be denied access unless a cardholder has override permissions assigned to their access group.
- **Anti-passback**: Not available with offline use.

To create a door mode profile

1 From the Explorer Bar's Navigator tab, click the Time & Mode Profile icon.

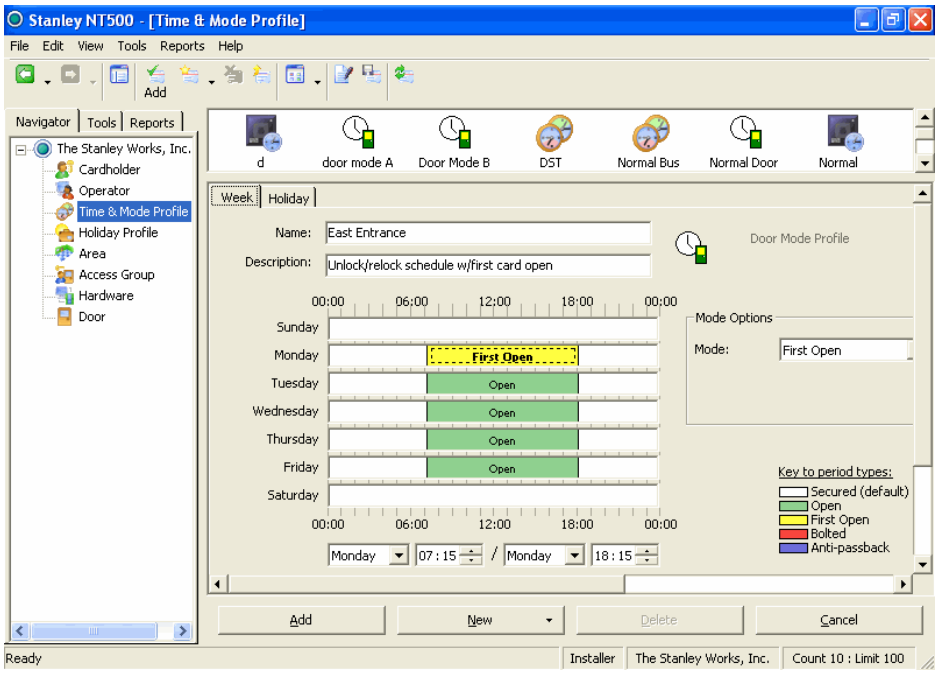
2 From the main menu click Edit > Create New Record.

3 Click Create New Door Mode Profile.

The Door Mode Profile window appears.

Notes

Figure 3.14 Creating a door mode profile



4 In the Name field, enter a name for the door mode profile.

5 In the Description field, enter a description of the door mode profile.

6 The hours of access defined by this door mode profile can be selected by clicking in the white field next to each weekday label. Then, while holding down the left mouse button, highlight the range of desired times.

7 Select the mode option that will be used to define each time duration from the Mode Options drop-down list.

8 Click Add.

A new door mode icon appears at the top of the screen.

To update a door mode profile

1 Select an existing door mode profile.

The Door Mode profile window appears.

2 Edit the desire details.

3 Click Update.

To delete a door mode profile

1 Select an existing door mode profile.

2 Click Delete.

3 Click OK to confirm.

Notes

Creating a reader mode profile

Reader modes are used to define the security levels of dual validation readers.

Reader mode profiles offer the following mode options:

- Card (default)
- PIN only
- Card or PIN
- Card and PIN

To create a reader mode profile

1 From the Explorer Bar's Navigator tab click the Time & Mode Profile icon.

2 Click New > Create New Reader Mode Profile.

The Reader Mode window appears.

3 In the Name field, enter a name for the reader mode profile.

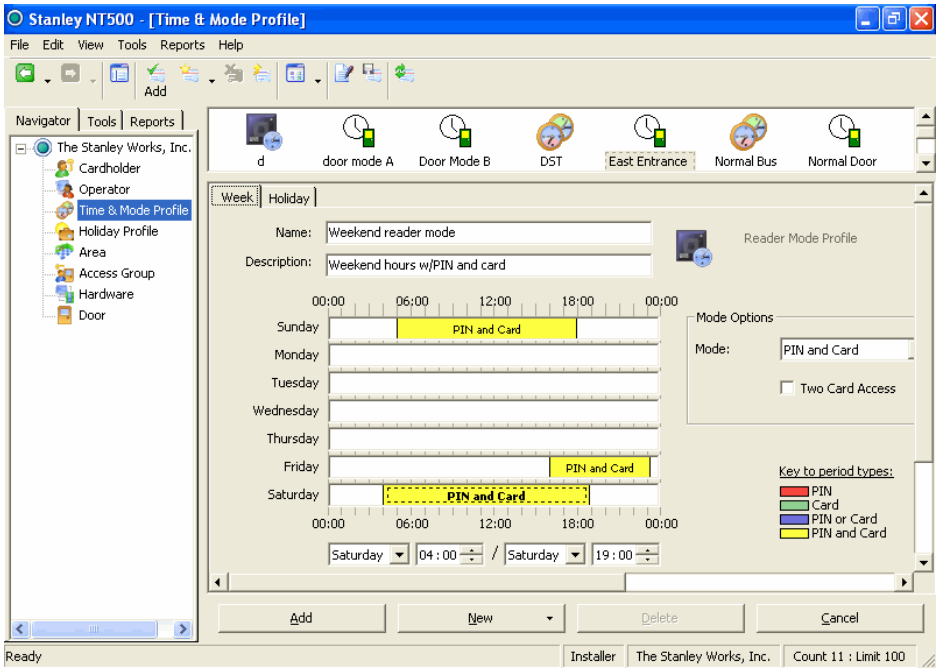
4 In the Description field, enter a description of the reader mode profile.

5 Select the hours for access by clicking in the white field next to each weekday label. Then, while holding down the left mouse button, highlight the range of desired times.

6 Select the mode option used to define each time duration from the Mode Options drop-down list. Click Add.

A new reader mode icon appears at the top of the window.

Figure 3.15 Creating a reader mode profile



Note: Mode options can be specified to require two-card access. In these instances, two cardholders must present cards to the reader in order to gain access.

To update a reader mode profile

1 Select an existing reader mode profile.
The Reader Mode window appears.

2 Edit the desired fields.

3 Click Update.

To delete a reader mode profile

1 Select an existing reader mode profile.
The Reader Mode window appears.

2 Click Delete.

3 Click OK to confirm.
The icon for the reader mode profile you deleted is no longer displayed in the window.

Notes

Notes

Area mode profile

Do not create area mode profiles for offline applications. We recommend assigning access based on areas (not doors) and based on groups rather than security levels. This access type is suggested because it allows you to add online functionality later if the needs of your site change. For more information about access types see page 3-13.

Setting up hardware

Now that access has been defined for specific times, locations, and/or cardholders, hardware information needs to be added to the database. The first type of hardware to be defined is a control panel. The AC301 Controller is a single door controller. The AC512 Controller has two door channels because it can control two doors. Each door channel can have one reader and a Request to Exit switch connected to it.

Adding a controller

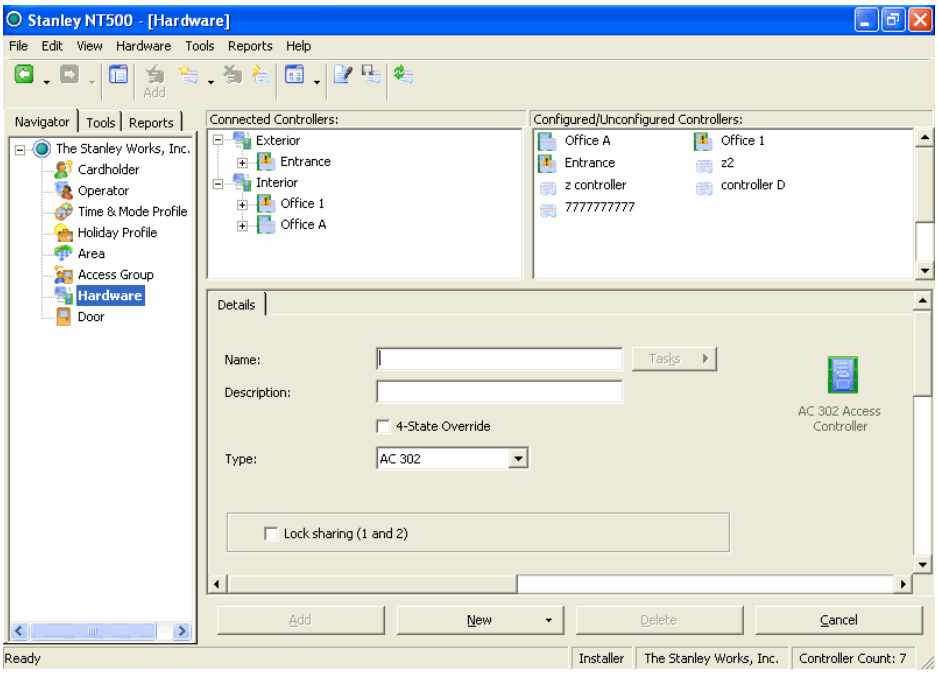
To add a controller

1 From the Explorer Bar's Navigator tab, click the Hardware icon.

2 From the main menu, click New > Create New Controller.
The Controller window appears.

Notes

Figure 3.16 Adding a controller



3 In the Name field, enter a name for the Controller.

4 In the Description field, enter a description of the Controller.

5 Select the controller type from the drop-down list. AC301 and AC512 are the only controllers applicable to an offline system.

6 Click the checkbox next to 4-State Override if this type of monitoring of the controller is used.

The 4-state circuit (fully supervised circuit) monitors the condition of the cabling as well as the activation circuit. This provides additional security to the override activation circuit and helps avoid an unnoticed trouble condition in the field wiring. A break in the wiring may not unlock the doors but instead will cause a supervisory condition to be reported to the software.

7 Click the checkbox next to Lock Sharing if the lock is controlled by an in and out reader on door channels n and m (specified by check box). This should only be used with 1100/2100 Series Door Controllers or Wiegand in and out readers.

8 Click Add.

A new controller icon appears in the window.

Notes

When a controller is added to the database, icons representing the number of door(s) that the controller can support appears in the door layout view.

Downloading the database to the controller can be accomplished via PDA or laptop. For instructions on using a laptop to download the database updates see page 3-40. See the *NT500 Transport Guide* for detailed instructions regarding use of a PDA and NT500 Transport software.

To update a controller

1 Select an existing controller.

2 Enter appropriate information.

3 Click Update to save your changes.

Updates to the controller can be downloaded from the database and then to a PDA or laptop for transfer. For instructions on using a laptop to download the database updates see page 3-40. See the *NT500 Transport Guide* for detailed instructions regarding use of a PDA and NT500 Transport software.

4 Download the new database to the controller.

To delete a controller

1 Select an existing controller.

2 Click Delete.

3 Click OK to confirm.

The icon for the controller you deleted no longer appears in the window.

Note: Deleting a controller deletes its associated doors.

Adding a channel

A door channel is the connection between a door and a controller. A channels must be associated with a controller such as the AC301 and AC512 controllers described above. Channels are required and provide a way to organize groups of doors to allow for ease of programming.

To add a channel

1 From the Explorer Bar's Navigator tab, click the Hardware icon.

2 From the main menu click New > Create New Channel.

The Channel details window appears.

3 In the Name field, enter a name for the Channel.

4 In the Description field, enter a description of the Channel.

5 The Channel Type field should read *Offline*.

6 The Protocol Type field should read AC300/500 Series RS232.

These two fields are not editable in offline mode.

7 Use the drop-down list to select the appropriate time zone.

8 Click Add.

Once a channel has been created, it can be assigned to a controller. The channel is the mechanism through which doors are then assigned to a controller.

To assign a controller to a channel

1 If not already viewing hardware, from the Explorer Bar's Navigator tab, click the Hardware icon.

Connected, configured, and unconfigured controllers as well as defined channels appear in the window.

2 To assign a controller to a channel, the controller icon can be dragged and dropped onto the channel icon.

a) Click on the controller icon for the controller to be assigned to a channel.

b) Holding down the left mouse button drag the icon to the left side of the window where channels icons are displayed.

c) Once the controller icon is situated over the channel icon release the left mouse button.

Notes

Notes

To remove a controller from a channel

1 Right click the controller.

2 Select Unconfigure Controller from the drop-down list.

With channels, controllers and their associated door(s) now represented in the access system database, doors can be assigned to specific areas. Doors and the areas they gate are linked in the database through the door details window.

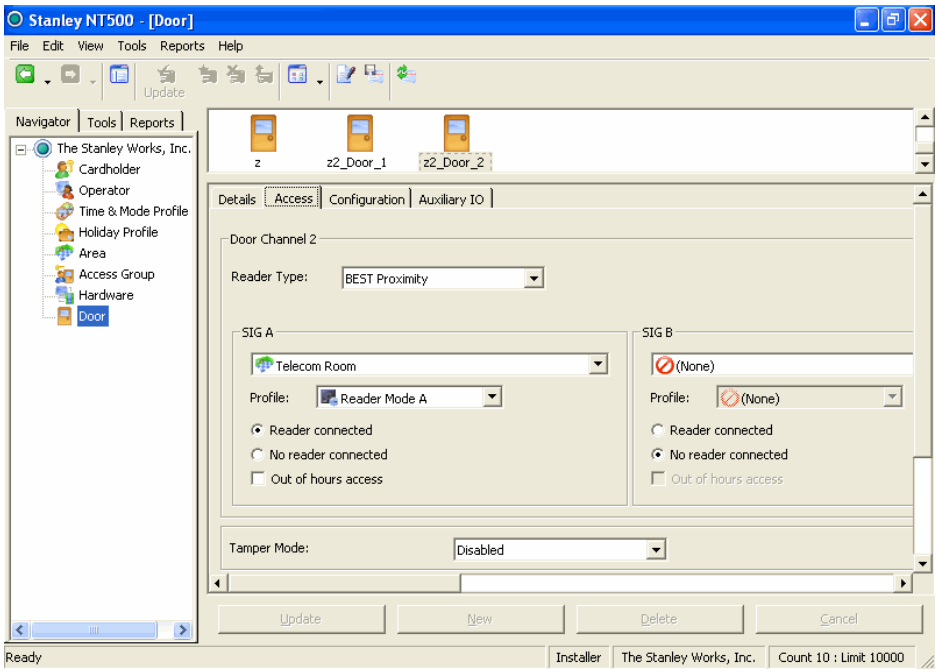
To associate doors and areas

1 On the Explorer Bar's Navigator tab, click the Door icon.

2 Select a door by double clicking on the appropriate door icon.

The Door Details window appears.

Figure 3.17 Adding door details



3 The door Name and Description can be modified if desired.

4 To assign a door mode profile to the door, select a door profile from the drop-down list.

5 To assign an area profile to the door, click the access tab.

6 Select a reader type from the drop-down list.

7 Select the areas gated by the door from the drop-down lists under SIG A and SIG B.

8 Click Update.

Notes

To update a channel

1 Select a channel.

2 Update the desired information.

3 Click Update to confirm your changes.

To delete a channel

1 Select a channel.

2 Click Delete.

3 Click OK to confirm.
The icon for the channel deleted no longer appears in the window.

Creating an access group

An access group is a way to organize multiple cardholders by granting members of the group access to specific areas. The access may be restricted by use of mode profiles.

To add an access group

1 From the Explorer Bar's Navigator tab, click the Access Group icon.

2 Click New.
The Access Group details window appears.

3 In the Name field, enter a name for the access group.

4 In the Description field, enter a description of the access group.

5 Click the Access tab.

6 Click the Profile 1 checkbox.

Access for the group can be defined in terms of time profiles and areas.

7 To apply a time profile select a time profile from the drop-down list.
When a time profile is applied to an access group it defines the access all members of that access group have.

8 To allow members of the group access to specific areas, click the appropriate check boxes from the areas listed.

9 If required, repeat for Profile 2.

Additional definition of controller options can be set on the Advanced tab.

Notes

To define additional controller options for an access group

1 Click the Advanced tab.

2 Check the desired options:

AC 300/500 Series Controller options

- Ignore bolted doors
- Ignore anti-passback
- Ignore dead bolted doors
- Ignore 'Two Card Access' mode

Note: Bolted mode denies access to all cards presented to the reader.

Conditional AC300/500 Series Controller options

- Allow passage mode
- Allow first card unlock

Note: Passage mode allows two swipes of a card to unlock the door indefinitely and then re-lock the same door when the card is presented twice to the reader again.

Note: Conditional options only apply when access is not controlled by airlock, anti-passback, area usage limits, or two-key access.

3 Click Add.

To update an access group

1 From the Explorer Bar's Navigator tab, click the Access Group icon.

2 Select an access group.

3 On the Details and Advanced tabs, enter the appropriate information.

4 Click Update to save changes.

To delete an access group

1 From the Explorer Bar's Navigator tab, click the Access Group icon.

2 Select an access group.

3 Click Delete.

4 Click OK to confirm.

The icon for the access group you deleted no longer appears in the window.

Creating cardholders and operators

Notes

Cardholders

A cardholder is a person who has a card. This could be a member of staff or a visitor. The card allocated to the cardholder is only valid for specified areas and times (e.g. visitors can be prevented from entering the Development area at any time and all areas after a certain date).

To add a new cardholder

1 From the Explorer Bar's Navigator tab, click the Cardholder icon.

2 Select New.

The Cardholder Details window appears.

3 Complete the Last Name and First Name fields on the Details tab.

4 Indicate Start Date, End Date, or Category if necessary.

5 Select each tab in turn and enter appropriate information.

6 Select Add.

A new cardholder icon appears at the top of the screen.

When viewing cardholder details the following information can be entered on the corresponding tab.

Title: The title of the cardholder (selected from a drop-down list).

Last Name: The last name of the cardholder (specified by data entry).

First Name: The first name of the cardholder (specified by data entry).

Initials: The initials of the cardholder (specified by data entry).

Start Date: The date and time the cardholder started employment or visiting (entered by data entry and drop-down calendar). Enabled/disabled by selecting its check box. If enabled, access is not allowed until the specified date and time but events (e.g an attempt to enter) are reported.

End Date: The date and time the cardholder ended employment or visiting (entered by data entry and drop-down calendar). Enabled/disabled by selecting its check box. If enabled, access is no longer allowed after the specified date and time but events (e.g an attempt to enter) are still reported.

Notes

Category: The category of the cardholder (selected from a drop-down list). The Customization facilities can be used to create/edit categories.

The category determines the format of the ID card.

Photo: A photo of the cardholder.

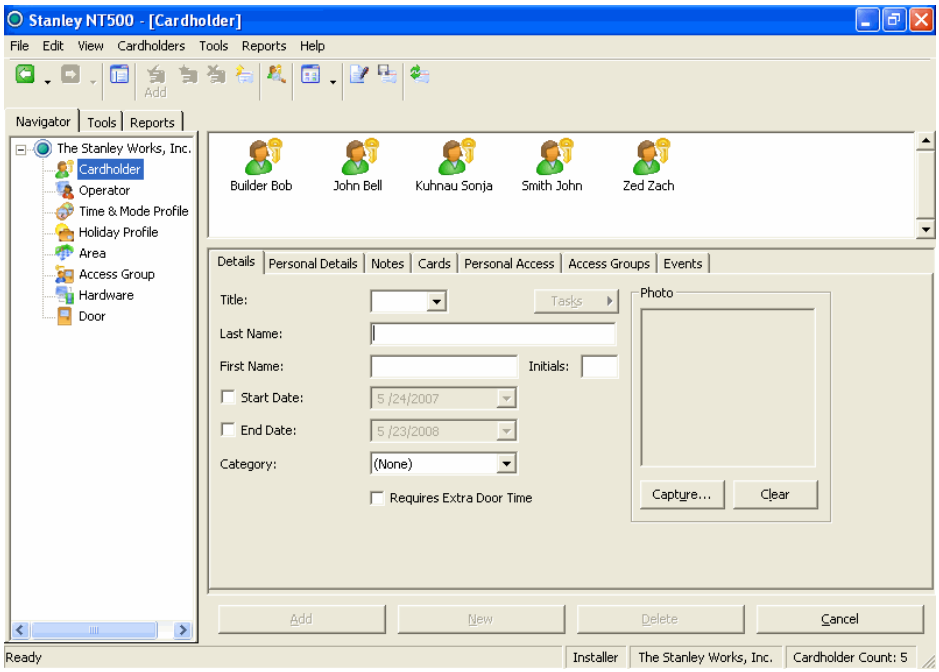
The photo can be captured from an image file, Twain device or Video device using the Capture button (see the Using the Capture Utility section).

A previously-captured photo can be cleared by selecting the Clear button.

A previously-created photo ID card for the selected cardholder can be printed by selecting the Print ID Card button. This requires the ID module. For further information, see the cardholder List View section.

Requires Extra Door Time: An indication of whether the cardholder requires extra time to get through the door (specified by check box). This feature is used to assist persons with mobility challenges.

Figure 3.18 Adding a cardholder



To assign a card and PIN to a cardholder

1 On the Cards tab, click Add New Card.

2 In the Card Format field, select the card format by using the drop-down list.

Notes

3 The card number can be manually entered or automatically populated if an office admin kit is being used.

4 Enter the Issue code.

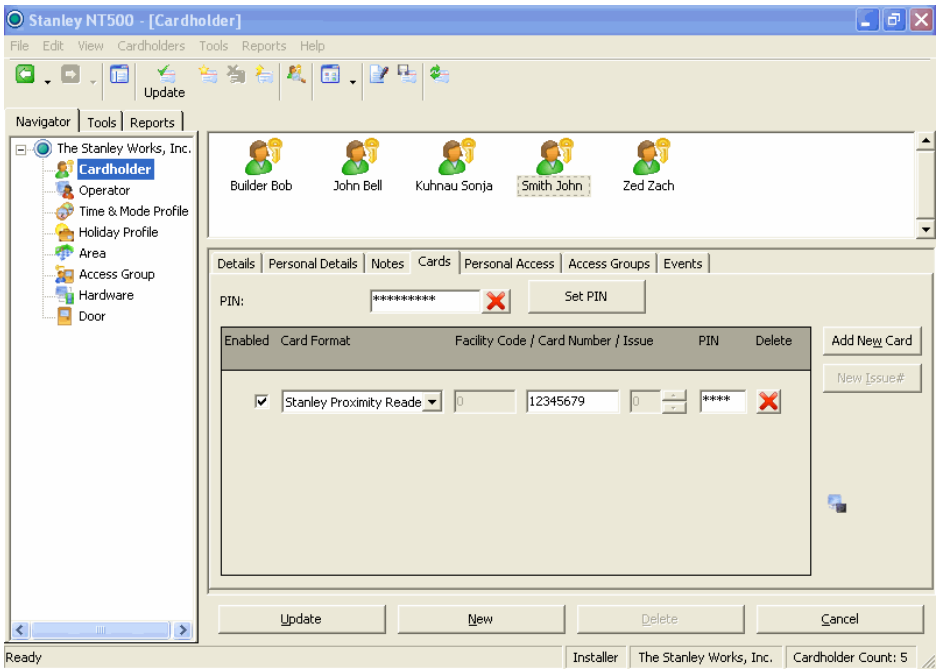
5 On the Cards tab, click Set PIN.

6 Enter a PIN number (up to 9 digits long) and confirm.

7 Click OK.

Note: If only PIN numbers will be used for access control, it is important not to duplicate PIN numbers in the database. If duplication occurs, there is no way to specifically identify who gained access to an area. To avoid this potential issue, it is recommended that all PIN numbers be assigned to a unique card number. Since duplicate card numbers are not permitted by the software, this will help prevent accidental PIN duplication. With a PIN only system, you must enter the PIN number as well as a card using the same PIN number as the card number.

Figure 3.19 Assigning a card and PIN



To define cardholder personal access details

1 Select the Personal Access tab.

2 Click the Profile 1 checkbox.

3 Select the time profile from the drop-down list.

Notes

Selecting 'None' allows access to the selected areas at all times.

4 Click the checkboxes next to the time profiles to specify the areas the time profile applies to.

5 If required, repeat for Profile 2.

To assign cardholder access group details

1 Select the Access Groups tab.

2 Select the access group(s) that cardholder belongs to.

3 Select Add on the Property Page.

To update a cardholder

1 Select a cardholder.

2 Select each tab in turn and enter appropriate information.

3 Click Update to save changes.

To delete a cardholder

1 Select a cardholder.

2 Select Delete.

3 Select OK to confirm.
The cardholder icon no longer appears in the window.

Operators

An operator is a cardholder who is allowed to make changes to the database determined by the operator privileges. For example, the receptionist in an organization may be allowed to add cardholders but not controllers or doors.

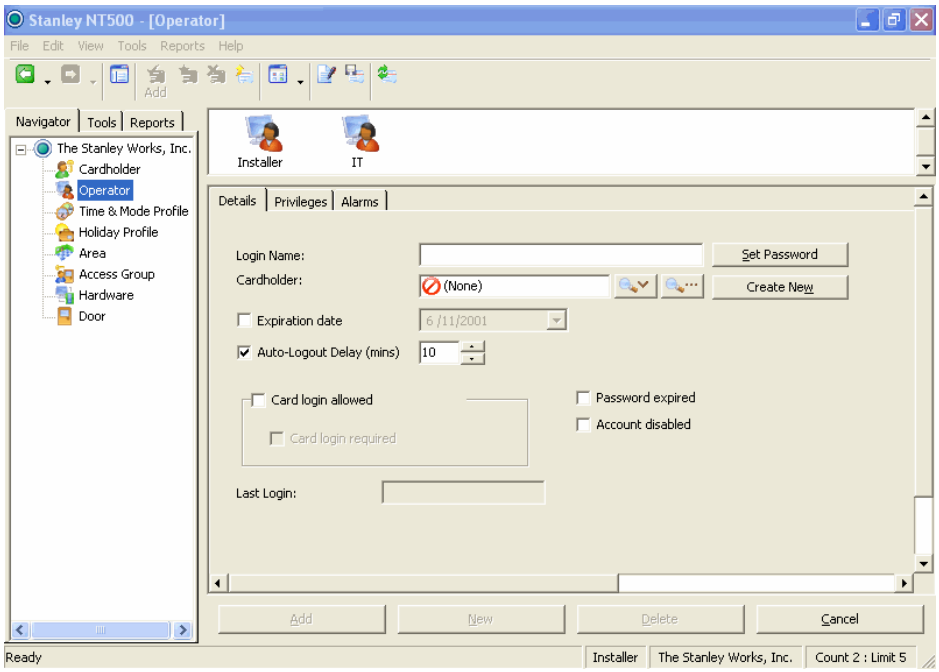
To add an operator

1 From the Explorer Bar's Navigator tab, click the Operator icon.

2 Select New.

The Operator window appears.

Figure 3.20 Adding an operator



3 Select each tab in turn and enter appropriate information.

4 Click Add.

When viewing operator details the following information can be entered on the corresponding tab.

Login Name: The type of user (specified by data entry). Specify a password for the user by selecting Set Password.

Cardholder: The cardholder who is also an operator (specified by searching for an existing cardholder or selecting Create New and creating a new cardholder). A cardholder can only be assigned one set of operator privileges per organizational unit.

Notes

Notes

Expiration Date: The date the operator privileges will be removed from the cardholder if the Password Expired check box is selected (specified by data entry and drop-down calendar).

Auto-Logout Delay (minutes): If selected, the operator will be logged out automatically if the system is not used for the specified time (range 1 to 120 minutes, specified by checkbox and data entry or increments).

Note: If this value is changed, the updated value takes affect after the next login.

Card Login Allowed: An indication of whether a card can be used to login (specified by check box).

Card Login Required: An indication of whether a card must be used to login (specified by check box).

Password Expired: An indication of whether the password has expired and a new password must be specified (specified by check box).

Account Disabled: An indication of whether the user is prevented from logging in (specified by check box).

Last Login: The date of the last login (automatically entered).

To set a password

1 From the Operator Details tab, click Set Password.
The Set Password window appears.

2 Enter the new password (at least 6 characters) and confirm password.

3 Click OK.

Operator privileges

Operator privilege levels allow for common pre-defined groups of software access to be assigned to individual operators. Potential operator privileges include:

No privileges: Cannot access the organizational unit.

Guest Administrator: Read access to cardholders.

Guest: Read access only. No access to Database Backup, Alarm Viewer, Alarm Map Designer, Event to Action, Card Designer, Event Archiving, and Audit Trail.

Monitor: Event log facilities and read only access to time profiles, holiday profiles, areas, channels, controllers and doors.

Guard: Alarm Viewer only and no auto-logout.

Manager: Read access to all facilities except Operators; plus write access to cardholders and add access to event archiving.

Security Manager: Read access to all facilities except Operators, Event Archiving and Audit Trail; plus write access to cardholders, access groups, areas, time/mode profiles, holiday profiles.

Operator: Write access to all facilities except Hardware, Alarm Map Designer, Card Designer, Event to Action and Audit Trail.

Supervisor: Write access to all facilities.

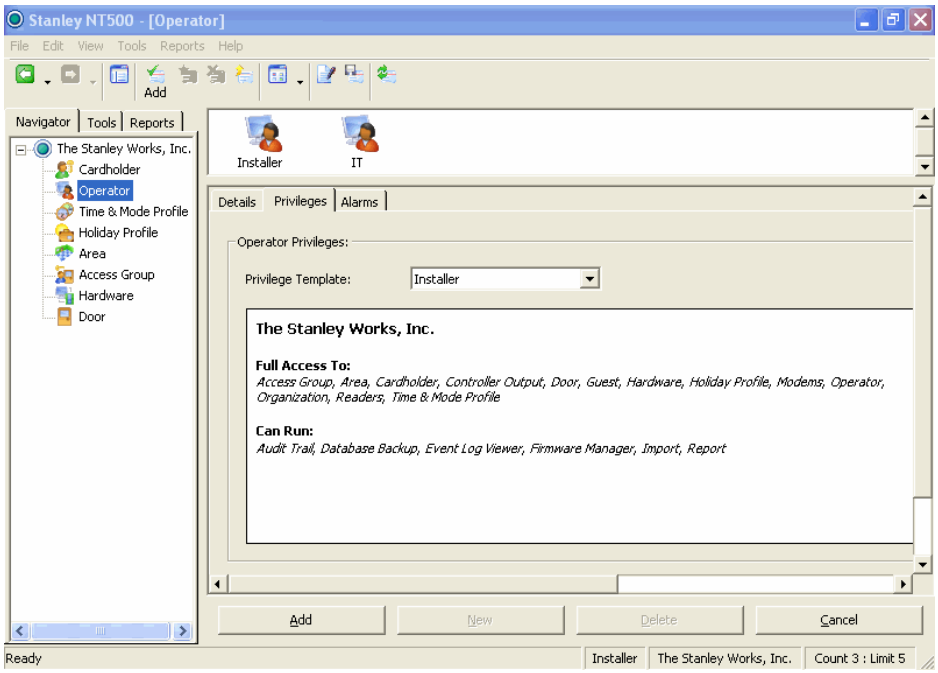
Installer: Write access to all facilities except Hardware.

Notes

To display and allocate operator privileges

1 Click the Privileges tab of the Operator window.

Figure 3.21 Allocating operator privileges



2 If multiple organizational units exist, select the Organization.

Note: Organizational units are a means of segregating the NT500 database into logical units which enables sites to be managed separately. It prevents unnecessary controller downloads and prevents operators from editing sites which they should not have any jurisdiction.

Notes

3 Select a Privilege Template from the drop-down list:
- No privileges
- Guest Administrator
- Guest
- Monitor
- Guard
- Manager
- Security Manager
- Operator
- Supervisor
- Installer

Note: If specifying an installer or supervisor, system customization is only allowed if installer/supervisor privileges are given to all organizational units.

4 Repeat steps 1 through 6 for each organizational unit (*No privilege* is the default).

Configuring a lock using a laptop

The lock can be configured using a laptop or PDA. See the *NT500 Transport Guide* for detailed instructions regarding use of a PDA and NT500 Transport software. To configure a lock using a laptop, use the following steps.

To connect to a lock using Stanley NT500 Software, the following items are necessary:

- Laptop running Stanley NT500, with a serial port or a USB to serial cable
- Null modem adapter
- Programming cable for connecting NT500 Locks to the serial port or serial cable (BEST part number C63290)
- Temporary operator card for NT500 Locks (provided with the locks).

To connect the laptop to the lock

1 If your laptop does not have a serial port, connect a USB to serial cable to the USB port on the laptop.

2 Connect the programming cable to the serial port or serial cable.

3 Connect the programming cable to the lock's communication port. The connector snaps in place.

To identify and configure a lock

To identify and configure a lock the laptop must be connected properly to the lock. The Stanley NT500 Software is used to choose the appropriate controller information to transfer.

1 From the Explorer Bar's Navigator tab, click the Hardware icon.

2 Under Connected Controllers, highlight the controller you want to configure.

3 Identify the controller:

a) On the Details tab, click Tasks, then Identify Controller…

The *Identify/Configure Controller* window appears.

b) In the COM Port field, select the appropriate COM port.

c) Click Identify.

A message appears stating, "Please check the connection or wake the controller."

d) Swipe a temporary operator card to activate the lock.

The diagnostic information for the lock appears.

4 Click Configure.

A message appears stating, "Connect 'Controller Name' with 'Serial Number'?"

5 *Click OK.*

The controller is now configured with the diagnostic information from the lock.

To transfer controller settings to a lock

When a connection is made to the controller to allow transferring controller settings, events will be automatically updated first. Then the task of transferring settings can be selected.

1 Make sure the laptop is connected to the lock.

2 From the Explorer Bar's Navigator tab, click the Hardware icon.

3 Under Connected Controllers, highlight the controller with the settings you want to transfer to the lock.

4 Connect to the controller:

a) Click Tasks, then Connect to Controller.

The Connect to Controller window appears.

b) In the COM Port field, select the appropriate COM port.

c) Click Connect.

Notes

Notes

A message appears stating, "Please check the connection or wake the controller."

d) Swipe a temporary operator card to activate the lock.

A message appears stating, "Successfully connected to controller."

5 Click OK.

A message appears stating, "Events collection progress (100%)".

6 Click OK.

The event history is transferred from the lock.

7 Click Tasks, then Download controller database...

A message appears stating, "Download to 'Controller Name', are you sure?"

8 *Click OK.*

A message appears stating, "Controller database download (100%)".

9 *Click OK.*

The settings are transferred to the controller.

To transfer event history from the lock to Stanley NT500

1 Connect the laptop to the lock.

2 From the Explorer Bar's Navigator tab, click the Hardware icon.

3 Under Connected Controllers, highlight the controller whose information you want to transfer to the database.

4 Connect to the controller:

a) Click Tasks, then Connect to Controller.

The Connect to Controller window appears.

b) In the COM Port field, select the appropriate COM port.

c) Click Connect.

A message appears stating, "Please check the connection or wake the controller."

d) Swipe a temporary operator card to activate the lock.

A message appears stating, "Successfully connected to controller."

5 Click OK.

Notes

A message appears stating, "Events collection progress (100%)".

6 Click OK.

The event history is transferred from the lock to the Stanley NT500 application.

To reset the diagnostic code

1 Repeat Steps 1-6 from above (To transfer event history from the lock to Stanley NT500).

2 On the Details tab, click Tasks, then Reset diagnostic code.

The diagnostic code is reset and a message appears stating, "Diagnostic code reset for controller."

3 Click OK.

To disconnect from the lock

When you are finished performing tasks at the lock, do the following:

1 Click Tasks, then Disconnect from Controller.

A message appears stating, "Successfully disconnected from controller."

2 Click OK.

3 To disconnect the laptop from the lock, press the button on the programming cable connector and unplug the programming cable from the lock's communication port.

Configuring an office admin kit as an enrollment station

With NT500 you have the flexibility to use an office admin kit (admin reader) to assign cards to cardholders. An office admin kit can be connected to a controller via PC interface. This reader can then be used to assign cards to cardholders.

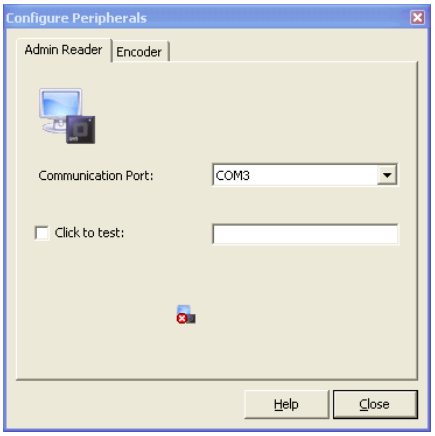
To configure the admin reader as an encoder

1 From the main menu, select Tools > Configure Peripherals.

The Configure Peripherals window appears.

Notes

Figure 3.22 Configure Peripherals window



2 Select the Admin Reader tab.

3 Select a communication port from the drop-down list. The port selected should correspond to the port via which the reader is connected to the PC.

4 Select the Click to test checkbox.

5 Present a card to the reader.

The card's code should be displayed on the screen.

To specify additional information for a MSR206 Magnetic Stripe card writer

1 Select the Encoder tab.

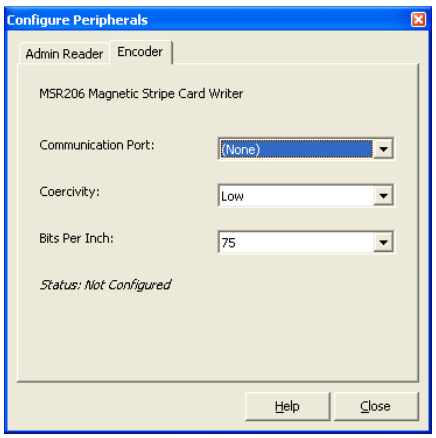
2 Select the PC communication port via which the reader is connected to the PC, using the drop-down list.

3 Select a coercivity level, using the drop-down list.

4 Select a bits per inch level, using the drop-down list.

5 Click Close.

Figure 3.23 Configure Peripherals - Encoder tab



Viewing events, diagnostic information, and reports

Notes

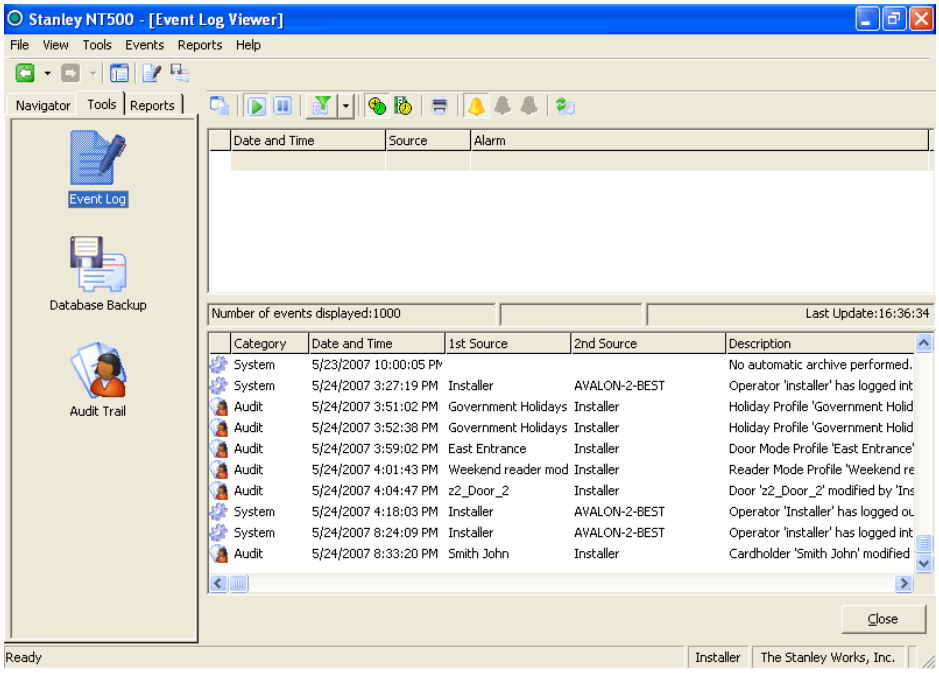
Viewing events

To view events

1 From the Explorer Bar's Tools tab, click the Event Log icon.
The filter functionality can be used to exclude specific event types from the event log.

2 To utilize the filter, Click the Filter Icon or select Filter from the Tools Toolbar.

Figure 3.24 Viewing events


Stanley NT500 - [Event Log Viewer]
File View Tools Events Reports Help
Navigator Tools Reports
Event Log
Database Backup
Audit Trail
Date and Time Source Alarm
Number of events displayed:1000
Last Update:16:36:34
Category Date and Time 1st Source 2nd Source Description
System 5/23/2007 10:00:05 PM No automatic archive performed.
System 5/24/2007 3:27:19 PM Installer AVALON-2-BEST Operator 'installer' has logged int
Audit 5/24/2007 3:51:02 PM Government Holidays Installer Holiday Profile 'Government Holid
Audit 5/24/2007 3:52:38 PM Government Holidays Installer Holiday Profile 'Government Holid
Audit 5/24/2007 3:59:02 PM East Entrance Installer Door Mode Profile 'East Entrance'
Audit 5/24/2007 4:01:43 PM Weekend reader mod Installer Reader Mode Profile 'Weekend re
Audit 5/24/2007 4:04:47 PM z2_Door_2 Installer Door 'z2_Door_2' modified by 'Ins
System 5/24/2007 4:18:03 PM Installer AVALON-2-BEST Operator 'Installer' has logged ou
System 5/24/2007 8:24:09 PM Installer AVALON-2-BEST Operator 'installer' has logged int
Audit 5/24/2007 8:33:20 PM Smith John Installer Cardholder 'Smith John' modified
Close
Ready
Installer
The Stanley Works, Inc.

Using diagnostics features

Device diagnostic information can be retrieved using a PDA or laptop with NT500 Transport software installed. See the *NT500 Transport Guide* for details about downloading diagnostic information using a PDA.

Once diagnostic information has been downloaded from the lock it can be viewed on the NT500 PC but cannot be modified.

Diagnostic information

Serial Number: The serial number of the controller.

Firmware ID: The firmware identity of the controller.

Firmware Version: The current firmware in the controller.

Notes

Firmware Type: The type of firmware in the controller. Different types may provide different features.

Board Revision: The revision number of the printed circuit board of the controller.

Power Status: The status of the controller's power supply.

Battery Status: The status of the controller's battery.

Backup Battery Status: The status of the controller's backup battery.

Battery Level: The charge on the controller's battery.

Diagnostic Code: A 2-byte hexadecimal number that can be mapped to one or more diagnostic messages. Zero indicates that no diagnostic conditions exist.

To view diagnostic information

1 From the Explorer Bar's Navigator tab, click the Hardware icon.

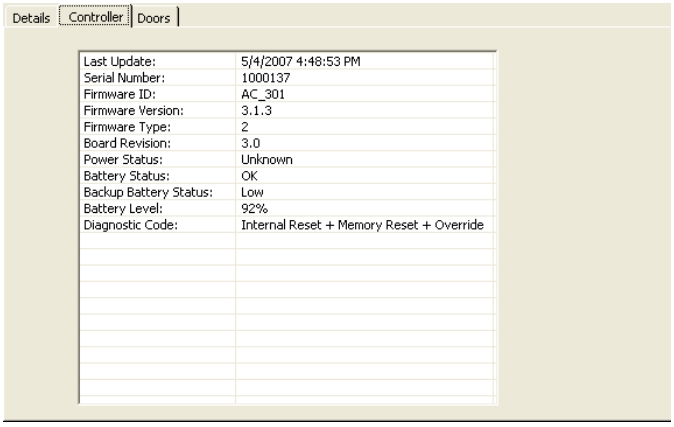
2 Select a controller.

The report details window appears.

3 Click the Controller Tab.

The device's diagnostic information is displayed .

Figure 3.25 Sample diagnostic information



Generating reports

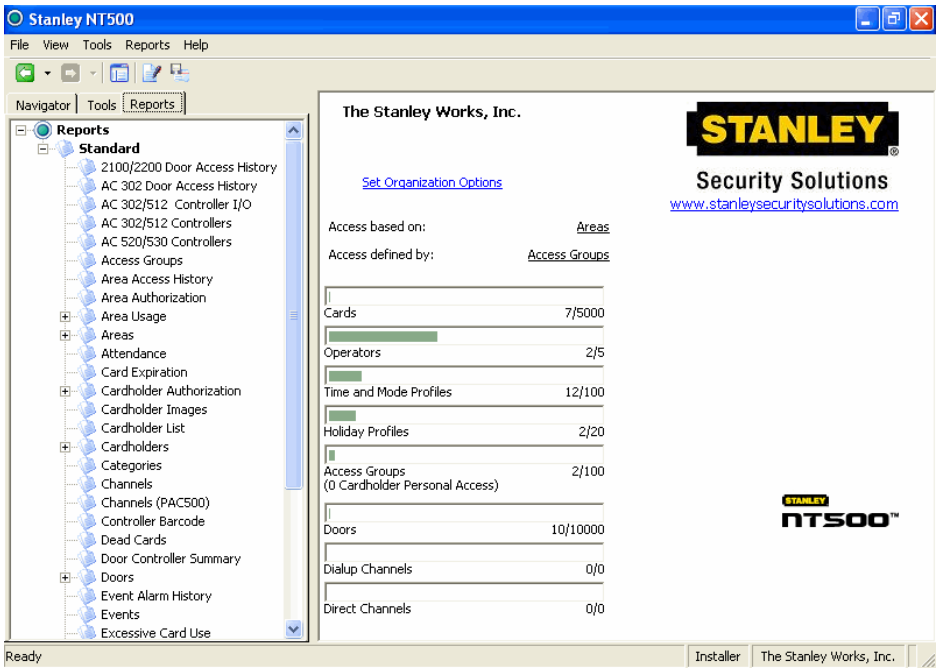
To generate a standard report

1 Click the Explorer Bar's Reports tab.

The Standard Reports List appears.

Notes

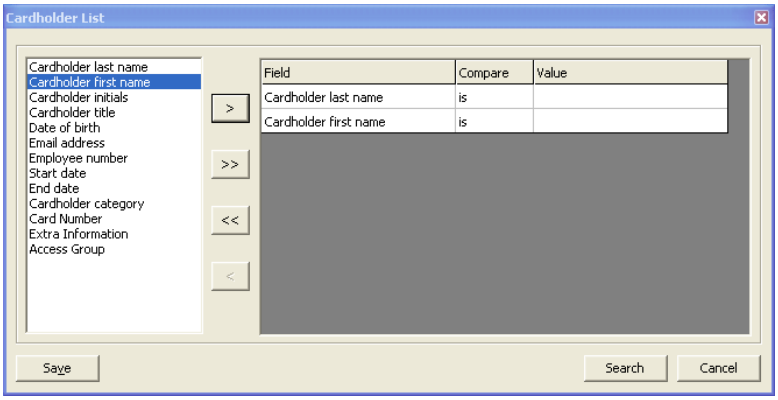
Figure 3.26 Standard reports list



2 Select a specific report from the options listed.

The report details window appears.

Figure 3.27 Report details window



3 Select the fields to be included in the report by highlighting the field name, then clicking the > icon.

4 To include all available fields in the report, select the first field in the list, then click the > > icon.

5 Click Save.

6 Name the search.

7 To see a preview of the output of a defined report, click Search.

A report preview appears

Notes

8 To print the report, click Print.

To print a saved report

1 Click the Explorer Bar's Reports tab.

2 Select a specific report from the options listed.
A report preview appears.

3 Click Print.

Database backup and restoration

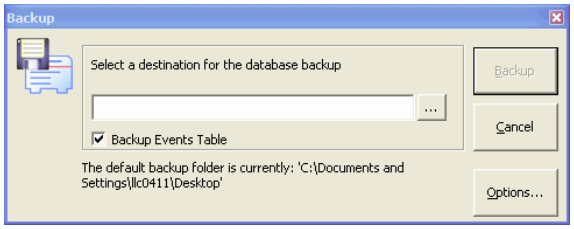
Notes

To backup the database

1 From the Explorer Bar's Tools tab, click the Database Backup icon.

The Backup window appears.

Figure 3.28 Database backup window



2 Click the ... icon to navigate to the desired destination for the database backup.

3 In the Filename field, enter a name for the backup file.

4 Click Save.

5 Click Backup.

A message appears when the database backup has been successfully created and saved.

Database restoration

A database restoration can only be performed by an Operating System Administrator.

To restore a NT500 Series database

1 Ensure that all users are logged off.

2 From the workstation desktop Click Start > Programs > NT500 Series Tools > Restore Database.

The Restore window appears.

3 Select a file using the browse facility.

4 Click the Restore button.

Upgrading licenses

To obtain a license key you must contact Stanley Security Systems Tech Support and provide a fingerprint.

Notes

To obtain a fingerprint from the NT500 System software sever

1 From the main menu click Tools > Upgrade License.

The license key window appears and the fingerprint is listed.

2 Record the fingerprint number and provide this information along with the license type needed (NT520, NT540, or NT550) to Tech Support.

You may locate the representative nearest you by visiting us on the web at www.stanleysecuritysolutions.com.

Tech Support will provide a license key.

3 After obtaining the license click on New License and enter the key provided to you.

Appendix A

Glossary of Terms

Notes

Terms

access group — A way to organize multiple cardholders by granting members of the group access to specific areas. The access may be restricted by use of mode profiles.

access level — An access control relationship made between a reader or readers and a time profile or time profiles. An access level is assigned to a card for the purpose of granting access through a reader or readers during a specified time.

activation/deactivation date — The date that a card becomes active or expires.

ActiveSync — A Microsoft utility designed to synchronize the data between a PC-based application and a PDA application. ActiveSync is used to synchronize the data between NT500 System software and NT500 Transport.

admin kit — See *office admin kit*.

admin reader — See *office admin kit*.

antipassback — A configuration limiting the ability of consecutive uses for a card at a reader. Usually, configured with readers installed on both the secure and non-secure side of an opening door. Once a card has been used in a reader to gain access on one side of the opening, the card cannot be used in the same reader until the card is used to gain access to a reader from the opposite side of the opening.

area — A space defined by a point of access that includes at least one door with an electronic lock managed by the NT500 System Software.

card — The card or token that carries a cardholder's data.

card ID — Part of the access control information that is encoded to a card. This information, usually numerical, is unique to a particular cardholder.

card format — The way that data is arranged and ordered on the card.

cardholder — An individual who is issued a particular card.

chassis type The designation that defines the physical lock type. Three types exist: cylindrical, mortise, or exit hardware. See those terms for more information.

coercivity The degree of magnetic force needed to encode a magnetic stripe card.

communication port The connector on the bottom of the NT500 Lock that allows the lock to be connected to a PDA running NT500 Transport.

communication server A module that allows communication between the database and door controllers.

controller A circuit board with on-board memory that is responsible for making most of the decisions in an access control system.

cylindrical Lock chassis that installs into a circular bore in the door.

diagnostic code The code in NT500 Transport that identifies the processing error.

encoder The device, connected to a PC running NT500 System software, used to encode magnetic stripe cards.

exit hardware Lock chassis type that supports the NT500 exit hardware trim lock.

extended unlock The extra period of time the lock will unlock when an authorized card with extended unlock privileges is presented.

facility code Part of the access control information that can be encoded to a card. This information, usually numerical, is unique to a group of cards.
Usually this feature is used to authenticate a card to a particular organization.

input A hardware connection point used for status reporting of a particular sensor.

Notes

Notes

issue code Part of the access control information contained on a card that allows reuse of the card ID when a card is lost, damaged, or stolen. Usually one or two digits in length, this code increments forward when creating a new card. Access is granted only when the card ID and the issue code match the current database information.

look ahead An offline feature where a higher issue code for a particular card ID knocks out the same card ID with a lower issue code from an offline lock when the card ID with higher issue code is presented to the lock.

mortise A lock chassis that installs into a mortised cavity in the edge of a door.

NT500 Transport The application that runs on a PDA designed to update NT500 locks and retrieve lock history.

office admin kit Magnetic stripe reader that when connected to a controller, via a PC running NT500 System Software, can be used as an encoder.

organizational units A means of segregating the NT500 database into logical units which enables sites to be managed separately. It prevents unnecessary controller downloads and prevents operators from editing sites which they should not have any jurisdiction.

output An NT500 on-board relay or switch that is configurable to follow the status of an input, system condition, or a time zone.

passage mode The ability to double present an authorized card within the strike time to unlock an opening. The lock is returned to its original status by a second, double presentation of an authorized card.

PDA Personal Digital Assistant.

programming cable The cable used to connect the PDA to the NT500 Lock.

request to exit A sensor usually installed on the non-secure side of the door that will mask the door position switch upon activation.

security level A security level can be assigned to a card to determine which doors it can open or areas it can access. A door or area is also assigned a security level and the security level of the card must be equal to, or greater than the security level of the door or area to allow access.

time interval A specific range of time, which corresponds to a particular day or days of the week. A time profile can be comprised of several, individual intervals.

time profile A defined range of time for assignment to various access control activities. A time profile may be applied to a reader or readers when creating an access level, to a reader to change the mode of operation, and a host of other operations.

two-card control The requirement for the presentation of two separate, authorized cards in order to gain entry through an access controlled opening.

unlock duration The time that the lock momentarily unlocks.

Notes